VIP'ContentManager

Administratorhandbuch

VERSION 5e.05

Gauss

Copyright © 1999-2001 Gauss Interprise AG Hamburg, Gauss Interprise, Inc. Irvine, California. Alle Rechte weltweit vorbehalten.

Dieses Dokument sowie die zugehörige Software sind Eigentum der Gauss Interprise AG oder ihrer Zulieferer und durch Gesetze zum Schutze des Urheberrechts und andere Gesetze geschützt. Sie werden unter einer Lizenz vertrieben, durch welche die Nutzung, Reproduktion, Vertrieb und Dekompilierung eingeschränkt wird. Weder der Erhalt noch der Besitz dieses Dokumentes ermächtigt Sie, dessen Inhalte ganz oder teilweise auf Papier, elektronisch oder einem anderen Medium zu reproduzieren, weiterzugeben oder anderen den Zugang darauf zu ermöglichen. Kein Teil dieses Dokumentes darf in irgendeiner Form und Weise ohne vorherige schriftliche Zustimmung der Gauss Interprise AG oder Gauss Interprise, Inc. reproduziert werden.

Obwohl bei der Erstellung der Dokumente sorgfältig vorgegangen wurde, können Fehler nicht ausgeschlossen werden.

Daher können Gauss Interprise AG, Gauss Interprise, Inc. sowie die Autoren keine Haftung für die Richtigkeit oder Vollständigkeit der in diesem Dokument enthaltenen Informationen übernehmen. Die Autoren sind für Hinweise über mögliche Fehler in den Dokumenten dankbar.

Darüber hinaus haften Gauss Interprise AG und Gauss Interprise, Inc. nur gemäß dem Lizenzvertrag der Software, die mit diesem Dokument verkauft wurde.

DIE DOKUMENTATION WIRD “WIE BESEHEN” GELIEFERT. SÄMTLICHE AUSDRÜCKLICHEN UND STILLSCHWEIGENDEN BEDINGUNGEN, ZUSICHERUNGEN UND GARANTIEN EINSCHLIESSLICH SÄMTLICHER GARANTIEN DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER DES NICHTVERSTOSSES GEGEN EIN GESETZ WERDEN ABGELEHNT, SOFERN NICHT EINE DERARTIGE ABLEHNUNG RECHTLICH ALS UNGÜLTIG ANGESEHEN WIRD.

SpyView, SpyImage, VIP’ContentManager, VIP’PortalManager und VIP’ContentMiner sind eingetragene Warenzeichen der Gauss Interprise AG und Gauss Interprise Inc. Alle anderen Produkte, Warenzeichen oder Handelsmarken, auf die in diesem Dokument Bezug genommen wurde oder die in diesem Dokument erwähnt wurden, sind Eigentümer der entsprechenden Firmen.

http://www.gaussinterprise.com

Programmversion: 5e.05

Dokumentenversion: De-05

Erscheinungsdatum: Mai 2001

Inhaltsverzeichnis

Abbildungsverzeichnis **6**

Tabellenverzeichnis **9**

Kapitel 1 Einleitung **11**

Kapitel 2 Überblick **17**

2.1 Systemarchitektur 17
2.2 Datei- und Verzeichnisstruktur 20

Kapitel 3 Installation **31**

3.1 Voraussetzungen 31
3.2 Installation der VIP-Server 33
3.3 Starten der VIP-Server 50
3.4 Migration von VIP 3.0 auf VIP 5e 50

Kapitel 4 Konfiguration **55**

4.1 Globale Arbeitsplatz-Voreinstellungen 55
4.2 Konfiguration des Webservers 59
4.3 Wiederherstellen einer früheren Objektversion 59
4.4 Zugriffsschutz 60
4.5 Konfiguration einer LDAP-Anbindung 76
4.6 Datenbankanbindung 88
4.7 Datensicherung 110
4.8 Konfiguration des SetExecutable-Agent 114
4.9 DiskSpace-Agent 115
4.10 Einstellen der Hauptspeicheranforderung 121

Kapitel 5 Arbeiten im Administrationssystem **123**

5.1 Anmelden im Administrationssystem 124
5.2 Website-Administration 126
5.3 Benutzer-Administration 133
5.4 Gruppen-Administration 142
5.5 Rollen-Administration 148
5.6 Systemadministration 154
5.7 Datenabgleich mit dem LDAP-Server 160

5.8 Funktionsbereiche 163

Kapitel 6 Zugriffskontrolle 169

6.1 Objektspezifische Zugriffsrechte 170
6.2 Vererbung von Zugriffsrechten 171
6.3 Standardmäßige Zugriffsrechte 174
6.4 Vorrangsregeln 175
6.5 Zugriffsrechte einstellen 177
6.6 Aufgabenspezifische Zugriffsrechte 184
6.7 Benutzer, Gruppen und Rollen 187
6.8 Tips 190
6.9 FAQs (Häufig gestellte Fragen) 191

Kapitel 7 Arbeiten mit dem VIP'DBC Editor 197

7.1 Tabellen anlegen und bearbeiten 197
7.2 VIP'DBC Formattabellen 203

Anhang A DefaultContent-Agent 209

A.1 Konfiguration 210
A.2 Arbeiten mit dem DefaultContent-Agenten 212

Anhang B HTMLConverter-Agent 217

B.1 Installation 218
B.2 Konfiguration 219
B.3 Funktionsweise 227
B.4 Testprogramm 231

Glossar 235

Index 239

Abbildungsverzeichnis

Abb. 1 – Architektur des VIP'ContentManager im Überblick 18
Abb. 2 – Aufgaben der Serverprozesse 20
Abb. 3 – Die Verzeichnisstruktur auf Server-Ebene 21
Abb. 4 – Die Dateistruktur des Pflegeservers 22
Abb. 5 – Die Struktur des Administrationsservers 25
Abb. 6 – Verzeichnisstruktur einer Website 25
Abb. 7 – Inhalte befinden sich im Verzeichnis WebSite 27
Abb. 8 – Allgemeine Einstellungen für die VIP-Installation 34
Abb. 9 – Installationseinstellungen 35
Abb. 10 – Beispiel einer verteilten Installation auf mehreren Server-Computern (Hosts) 40
Abb. 11 – Zugriffsschutzkomponente im Überblick 61
Abb. 12 – Microsoft Management Konsole (MMKS) 69
Abb. 13 – MMKS: Verzeichnissicherheit 70
Abb. 14 – MMKS: ISAPI-Filter 71
Abb. 15 – VIP'DBC Systemüberblick 91
Abb. 16 – Einrichten einer ODBC-Systemdatenquelle 102
Abb. 17 – Speicherstrategie mit Verdrängung 109
Abb. 18 – Beispielkonfiguration mit DiskSpace-Agenten auf dem Pflegeserver 116
Abb. 19 – Konfiguration der Server auf verschiedenen Rechnern 116
Abb. 20 – Konfiguration der Systeme mit separatem Produktionsserver 117
Abb. 21 – Die Startseite des VIP-Systems 124
Abb. 22 – Anmeldedialog für das Administrationssystem 125
Abb. 23 – Panel der Website-Administration 127
Abb. 24 – Dialog zum Anlegen einer neuen Website 128
Abb. 25 – Zuordnung von Website-Administratoren 129
Abb. 26 – Dialog zur Zuordnung von Gruppen zu einer Website 130
Abb. 27 – Dialog zur Zuordnung von Rollen zu einer Website 131
Abb. 28 – Dialog zur Zuordnung von Benutzern zu einer Website 132

Abb. 29 – Dialog der Benutzer-Administration 133
Abb. 30 – Dialog zum Anlegen eines neuen Benutzers 134
Abb. 31 – Dialog zum Zuordnen von Gruppen 137
Abb. 32 – Dialog zur Voreinstellung der Benutzerrechte 139
Abb. 33 – Dialog zur Gruppen-Administration 142
Abb. 34 – Dialog zum Anlegen einer neuen Gruppe 143
Abb. 35 – Dialog zum Bearbeiten einer Gruppe 145
Abb. 36 – Dialog für die Zuordnung von Benutzern zu einer Gruppe 145
Abb. 37 – Dialog zur Voreinstellung der Zugriffsrechte 147
Abb. 38 – Dialog zur Rollen-Administration 148
Abb. 39 – Dialog zum Einrichten einer neuen Rolle 149
Abb. 40 – Dialog zum Bearbeiten einer Rolle 150
Abb. 41 – Dialog für die Zuordnung von Benutzern zu einer Rolle 151
Abb. 42 – Dialog zur Voreinstellung der Zugriffsrechte 152
Abb. 43 – Dialog zur Systemadministration 154
Abb. 44 – Aktionsliste nach Benutzern sortiert 155
Abb. 45 – Dialog zum Beenden der Server 155
Abb. 46 – Dialog zum Abbrechen von langwierigen Aktionen 156
Abb. 47 – LDAP-Panel des VIP-Administrationssystems 161
Abb. 48 – Ergebnis der Abgleichprüfung mit LDAP 162
Abb. 49 – Workflow bei direkter Freigabe 164
Abb. 50 – Vererbung von Zugriffsrechten 172
Abb. 51 – Geänderte Zugriffsrechte 173
Abb. 52 – Wiederherstellen der vererbten Zugriffsrechte 174
Abb. 53 – Zugriffsrechte aufgrund der Gruppen- und Rollenzuordnung 176
Abb. 54 – Gruppen-, rollen- und benutzerspezifische Zugriffsrechte 177
Abb. 55 – Dialog zur Einstellung der Zugriffsrechte 179
Abb. 56 – Dialog zum Zuordnen einer Gruppe 180
Abb. 57 – Einstellungsmöglichkeiten für einzelne Zugriffsrechte 181
Abb. 58 – Zugriffsrechte für Pflege, QS und Produktion 185
Abb. 59 – Zuordnung von Benutzern zu Gruppen und Rollen 188

Abb. 60 – Zugriffsrechte zum Verschieben einer Seite 192
Abb. 61 – Der VIP'DBC Editor 198
Abb. 62 – Dialog zur Suche nach Tabellen 201
Abb. 63 – Der Formattabellen-Editor 203
Abb. 64 – Verweis auf eine andere Spalte im Formattabellen-Editor 207
Abb. 65 – Vorlagen im Thema "Templates/Projekte" 212
Abb. 66 – Inhaltsvorlagen im Thema "Inhaltsvorlagen/Projekte" 213
Abb. 67 – Der automatische Konvertierungsprozeß 228
Abb. 68 – Die Option *generieren mit Konverter* im Dialog *Neues Objekt anlegen* *230*
Abb. 69 – Das Attribut "Converter" 231

Tabellenverzeichnis

Tabelle 1 – Typographische Konventionen 15
Tabelle 2 – Properties-Dateien von VIP 23
Tabelle 3 – Attribute im Directory-Server 78
Tabelle 4 – Dateiangabe unter Windows NT und Unix 158
Tabelle 5 – Funktionsbereiche und Objekte 163
Tabelle 6 – Funktionen und erforderliche Zugriffsrechte 186
Tabelle 7 – Einträge in der Datei **converter.properties** 220
Tabelle 8 – Zusätzliche Angaben für den Eintrag `validExtensions` 223

KAPITEL 1

Einleitung

Aktuelle Technologie-Trends deuten darauf hin, daß Internet-Technologien (IT) die Basis künftiger Software-Anwendungen sein werden. Bei neueren Standard-produkten ist dies bereits erkennbar. Außerdem wächst bei den meisten IT-Anwendern das Bedürfnis nach Integration der vorhandenen Lösungen zu ganzheitlichen und damit prozeßorientierten IT-Anwendungen. Der Zwang zu integrierten Anwendungen ergibt sich auch aus den immer flacher werdenden Hierarchien und den erweiterten Verantwortungsbereichen der Mitarbeiter eines Unternehmens.

Es zeichnet sich ab, daß Webbrowser eine der wichtigsten Benutzerschnittstellen der Zukunft bilden werden (Stichwort: “Universal Client”). Die Benutzeroberflächen werden als HTML-Seiten oder Java-Applets entwickelt und vereinheitlichen so die Bedienung vielfältiger IT-Anwendungen. Daraus ergeben sich deutliche Vorteile in der Benutzung. Es wird eine prozeßorientierte Sicht auf die gesamte Landschaft der IT-Anwendungen eines Unternehmens möglich. Basierend auf dieser Erkenntnis wurde die Produktplattform VIP – Versatile Internet Platform – entwickelt.

Wie bei jeder jungen und innovativen Technologie mangelt es oft an professionellen Methoden und Werkzeugen für den Aufbau der neuen IT-Strukturen. Wenn es um den Einsatz von neuen Technologien bei IT-Anwendern geht, steht aber gerade dieser Aspekt im Vordergrund. Ohne ein professionelles Managementsystem für den Aufbau und die Verwaltung von Website-Inhalten entsteht sehr schnell ein enormer Wildwuchs an Dateien und Verzeichnissen. Die Lösung heißt: Web Content Management. VIP bietet ein professionelles Web Content Management System, basierend auf modernster Technologie, das die Entwicklung neuer IT-Infrastrukturen optimal unterstützt. Durch den Einsatz des VIP’ContentManager werden Ordnung, Sicherheit, Qualität und Transparenz in Ihre neuen IT-Strukturen gebracht.

Hinweise zu dieser Dokumentation

Dieses Administratorhandbuch stellt die Komponenten und Funktionen des VIP-Systems aus der Sicht des Systemadministrators dar. Als Administrator eines VIP-Systems sollten Sie fundierte Kenntnisse in den folgenden Bereichen besitzen:

- Installation und Konfiguration eines HTTP-Servers (Webservers)
- Konfiguration von Kommunikationsschnittstellen
- Standardbefehle zur Systemadministration, etwa zur Einrichtung und Pflege von Verzeichnisbäumen und Dateien
- Bedienung und Konfiguration von Webbrowsern wie Netscape Communicator oder Microsoft Internet Explorer

Die meisten der hier beschriebenen Funktionen sind nur im Administrationssystem des VIP'ContentManager zugänglich. Eine Ausnahme bilden die Funktionen der Zugriffskontrolle, die zwar im Pflegesystem durchzuführen sind, jedoch aufgrund ihrer besonderen Bedeutung für die Verwaltung von VIP-Objekten den Aufgaben der Website-Administration zugerechnet wurden.

Die Inhalte des Handbuchs sind folgendermaßen gegliedert:

- Kapitel 2 "Überblick" gibt Ihnen einen Überblick über die Architektur und die Verzeichnisstruktur eines VIP-Systems.
- Kapitel 3 "Installation" beschreibt die Installation der VIP-Server sowie den Startvorgang für die Serverprozesse.
- In Kapitel 4 "Konfiguration" werden verschiedene Einstellungen zur Konfiguration der VIP-Server sowie der Client-Systeme beschrieben.
- Kapitel 5 "Arbeiten im Administrationssystem" erläutert die Aufgaben und Funktionen des Administrationssystems, insbesondere die Server- und Website-Administration sowie die Administration von Benutzern, Gruppen und Rollen.
- In Kapitel 6 "Zugriffskontrolle" werden die Grundlagen der Zugriffskontrolle sowie die Funktionen und Einstellungsmöglichkeiten der Zugriffskontrolle im Pflegesystem des VIP'ContentManager ausführlich erklärt. Eine Einführung in die Grundbegriffe der Zugriffskontrolle finden Sie im Benutzerhandbuch.

- Kapitel 7 “Arbeiten mit dem VIP’DBC Editor” beschreibt die Bedienung des VIP’DBC Editors, mit dem man Datenbanken oder -tabellen als Datenquellen für das VIP-System einbinden kann.
- Anhang A “DefaultContent-Agent” behandelt den DefaultContent-Agenten.
- In Anhang B “HTMLConverter-Agent” werden die Funktionsweise und die Konfiguration des HTMLConverter-Agent beschrieben.

Neue Funktionen in Version 5e

Neue Objekttypen

Der VIP’ContentManager unterstützt jetzt die Erstellung von dynamischen und interaktiven Web-Inhalten. Dadurch haben Sie die Möglichkeit, den Inhalt von Seiten der Website komplett oder teilweise während der Laufzeit zu erzeugen. Dafür stehen Ihnen verschiedene neue Objekttypen zur Verfügung, mit denen Sie z. B. JSP-, ASP- oder PHP-Seiten erzeugen können.

Desweiteren gibt es nun die Objekttypen MS Excel (.xls), MS PowerPoint (.ppt), MS Word (.doc), PDF und CGI-Skript, die Sie für die entsprechenden Dokumente auswählen können.

JavaServer Pages

Der VIP’ContentManager unterstützt jetzt die plattformübergreifende Technologie von Sun Microsystems für die innovative Erstellung dynamischer Web-Seiten.

Offline-Datenabgleich mit und direktes Einloggen am LDAP-Server

Der Datenabgleich mit dem LDAP-Server kann jetzt offline über Befehlszeilen auf Ebene der Command-Shell bzw. Eingabeaufforderung ausgelöst werden. Darüber hinaus können Sie mit einem Parameter festlegen, ob ein direktes Einloggen über den LDAP-Server oder über den VIP-Server erfolgen soll.

Nachträgliches Ändern von Objekttypen

Bestimmte Objekttypen können nachträglich geändert werden. So haben Sie jetzt z. B. die Möglichkeit, HTML-Objekte in JSP-Objekte umzuwandeln.

Ausgabe von Objektprotokollen in anderen Sprachen

Die Protokolle der Objekte können jetzt in Deutsch oder Englisch ausgegeben werden.

Kaskadierte Vorlagen

Der VIP'ContentManager unterstützt jetzt die Verwendung von kaskadierten Vorlagen (cascading style sheets=CSS).

Sanfter Server-Shutdown

In Version 5e werden die VIP-Server stufenweise heruntergefahren. Die auf den Servern laufenden Aktionen sind nach ihrer Priorität in Gruppen eingeteilt. Beim Herunterfahren der Server wird zuerst die Ausführung neuer Aktionen in der ersten Gruppe unterbunden, so daß die Aktionen dieser Prioritätsstufe nach und nach auslaufen. Wenn in einer Gruppe alle Aktionen beendet sind, laufen die Aktionen der nächsten Prioritätsstufe aus. Dies wird so lange wiederholt, bis alle Aktionen auf den Servern beendet sind.

Umwandlung von URLs in das RFC 2396-Format

Um auch auf Systemen mit anderssprachigen Zeichensätzen die einwandfreie Navigation durch die Websites zu gewährleisten, werden im VIP'ContentManager ab Version 5e Umlaute und ähnliche Zeichen in URLs gemäß dem Standard RFC 2396 abgebildet, verwaltet und ggf. umgewandelt.

Wiederherstellen einer früheren Objektversion

Sie haben jetzt die Möglichkeit, frühere Versionen eines Objekts wiederherzustellen.

Suche nach Objekten über die OID

In bestimmen Fällen kann es erforderlich sein, die Zugehörigkeit von OIDs zu den entsprechenden Objekten zu ermitteln. Der VIP'ContentManager bietet jetzt die Möglichkeit, die Suche nach einem Objekt über die OID mit Hilfe des Objektfilters bzw. Filtereditors durchzuführen.

Typografische Konventionen

Elemente der Benutzeroberfläche werden im Text folgendermaßen hervorgehoben:

Tabelle 1 – Typographische Konventionen

Element	Schriftart oder Symbol	Beispiele
Menüeinträge	*Menü ⟶ Eintrag*	*Datei ⟶ Anlegen*
Fenster, Dialoge, Feld- und Buttonbezeichnungen	*Fenstertitel* *Button*	*Neues Objekt anlegen* *Abbrechen*
Datei- und Verzeichnisnamen, Pfade etc.	**Dateiname** **Verzeichnisname**	Die Datei **server.properties** im Verzeichnis **C:\Programme\vip**
Variablen	{Variable}	**{VIP-Installationsverzeichnis}**

KAPITEL 2
Überblick

Dieses Kapitel liefert einen Überblick über die Systemarchitektur sowie die Datei- und Verzeichnisstrukturen des VIP-Systems.

Die Architekturbeschreibung soll Ihnen ein grundlegendes Verständnis für die Arbeitsweise des VIP'ContentManager vermitteln. Dieses Wissen ist insbesondere für die Installation und Konfiguration des Systems von Bedeutung.

Der strukturelle Überblick dient im wesentlichen dazu, die VIP-Komponenten in Ihrem System zu identifizieren. In diesem Bereich sollten in der Regel keine manuellen Eingriffe vorgenommen werden, da dies zum Funktionsverlust der VIP-Systeme führen könnte. Eine Ausnahme stellen die in Kapitel 4 "Konfiguration" beschriebenen Konfigurationsdateien dar.

2.1 Systemarchitektur

Der VIP'ContentManager ist vollständig in Java implementiert und zwar als multi-tiered Client/Server-Lösung. Im Intranet findet die Client/Server-Kommunikation über Socket-Verbindungen statt. Alle Aktivitäten zur Administration einer Website werden über diese Verbindungen abgewickelt. Lediglich der Transfer von HTML-Seiten geschieht über das HTTP-Protokoll, so daß der Webserver nur für die Übermittlung dieser Daten benötigt wird. Alle übrigen Aktivitäten werden durch den VIP-Server kontrolliert. Bei der Verbindung zum Internet findet die Client/Server-Kommunikation des VIP-Systems über HTTP-Tunneling statt, falls eine Socket-Verbindung nicht möglich ist.

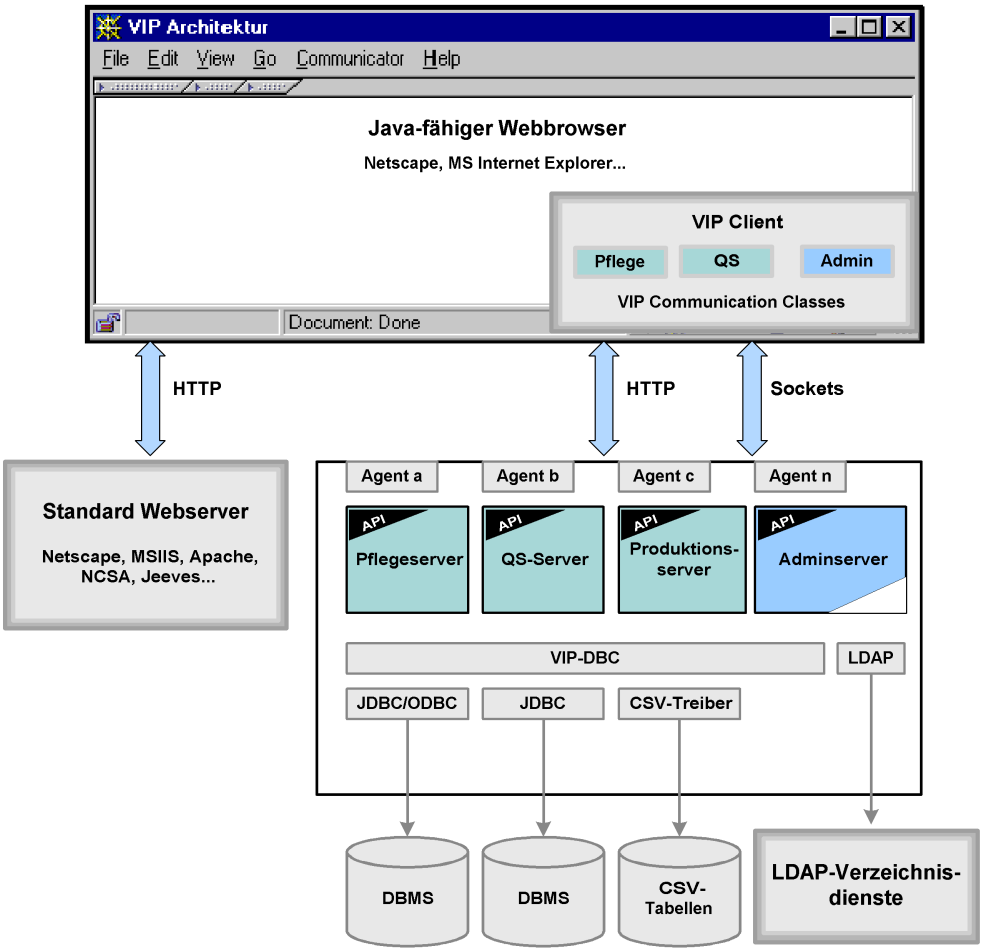

Abb. 1 – Architektur des VIP'ContentManager im Überblick

Datenbankschnittstelle

Über die integrierte Datenbankschnittstelle (VIP'DBC) greift das VIP-System auf externe Datenquellen zu. Sämtliche Verwaltungsdaten des VIP-Systems werden über die Datenbankschnittstelle abgelegt. Diese Daten können entweder in einem Datenbanksystem (DBMS) vorliegen – vorausgesetzt das DBMS bietet einen JDBC- bzw. ODBC-Treiber – oder als CSV-Tabellen.

Programmierschnittstelle

Durch die Programmierschnittstelle (API) der VIP-Server können Sie eigene Server-Klassen einbinden und damit eigene Agenten in den VIP'ContentManager integrieren. Über das API steht die gesamte Funktionalität des VIP-Systems zur Verfügung. Sämtliche Funktionen, die über die Benutzeroberfläche bedient werden können, sind auch über das API erreichbar. Weitere Informationen zum Server-API finden Sie in der Java'API-Dokumentation.

LDAP

Das Administrationssystem des VIP'ContentManager bietet die Möglichkeit, die Benutzer-, Gruppen- und Rolleninformationen eines LDAP-kompatiblen Verzeichnisdienstes einzubinden und im VIP-System zu nutzen. Dadurch kann der Verwaltungsaufwand für die Konfiguration und Pflege von Benutzerdaten erheblich reduziert und die unternehmensweite Konsistenz dieser Daten verbessert werden.

Serverprozesse

Durch das Workflowkonzept des VIP'ContentManager werden die Daten einer Website gleichzeitig durch die verschiedenen Server bereitgestellt und verwaltet. Hierbei handelt es sich um eigenständige Serverprozesse, die unabhängig voneinander gestartet werden können. Durch die Anmeldung an einem der VIP-Systeme nimmt ein Client Verbindung mit dem entsprechenden Serverprozeß auf.

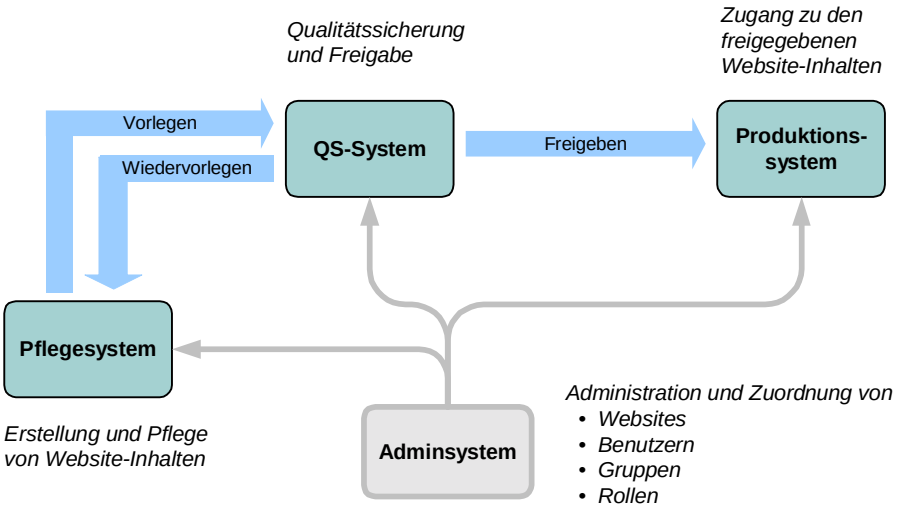

Abb. 2 – Aufgaben der Serverprozesse

- Durch das Pflegesystem werden alle redaktionellen Aufgaben bei der Erstellung und Pflege von Website-Inhalten verwaltet.
- Das QS-System verwaltet alle Daten, die zur Qualitätssicherung vorgelegt worden sind.
- Das Produktionssystem verwaltet die “publizierten” Daten einer Website und den “öffentlichen Zugang” zu diesen Daten.
- Das Adminsystem übernimmt alle Administrationsaufgaben wie das Anlegen von Websites, die Benutzerverwaltung usw.

2.2 Datei- und Verzeichnisstruktur

In diesem Abschnitt wird zunächst die logische Struktur beschrieben, in die sich ein vollständig installiertes VIP-System untergliedert. Manuelle Modifikationen in den hier beschriebenen Dateien und Verzeichnissen dürfen generell nicht vorgenommen werden. Trotzdem ist es notwendig, den exakten Aufbau zu kennen, um bei Problemen die Fehlerquelle qualifiziert eingrenzen zu können.

Abb. 3 – Die Verzeichnisstruktur auf Server-Ebene

Wenn das VIP-System mit den Standardinstallationseinstellungen installiert wird, befinden sich alle beschriebenen Verzeichnisse im Verzeichnis **\vip**.

Die Verzeichnisstruktur der drei Server für Pflege, Qualitätssicherung und Produktion ist nahezu identisch und wird im folgenden Abschnitt am Beispiel des Pflegeservers erläutert, wobei auf die Unterschiede zwischen den einzelnen Servern hingewiesen wird. Der Administrationsserver unterscheidet sich aufgrund der gesonderten Funktionalität. Weitere Informationen dazu finden Sie im Abschnitt “Dateistruktur des Administrationsservers” auf Seite 24.

Der Zugang zum Administrationssystem ist nur mit der Benutzerkennung “admin” möglich. Zum Pflege- und Qualitätssicherungssystem haben sämtliche Benutzer Zugang, die selbst einer Website zugeordnet sind, oder einer der Website zugeordneten Benutzergruppe bzw. Benutzerrolle angehören.

Im Hauptverzeichnis jedes Systems – außer dem Produktionsserver – ist die HTML-Seite **index.htm** enthalten (z. B. **{VIP-Installationsverzeichnis}\vip\edit\index.htm**), die bei jedem Start des jeweiligen Servers angezeigt wird. Diese Seiten dürfen auf keinen Fall geändert oder umbenannt werden.

Dateistruktur des Pflegeservers

Abb. 4 – Die Dateistruktur des Pflegeservers

- **Backup:** Dieses Verzeichnis enthält für jede Website ein entsprechendes Unterverzeichnis, unter dem die älteren Versionsstände der Website-Objekte (älter als die Vorgängerversionen der aktuellen Objekte) gespeichert werden. Siehe dazu den Abschnitt “Speicherung von Website-Objekten” auf Seite 28.
- **config:** In diesem Verzeichnis befinden sich die Konfigurationsdateien des jeweiligen Servers. Diese Dateien haben die Endung **.properties** und werden vom VIP-Server automatisch generiert. Die meisten dieser Konfigurationsdateien unterliegen der Verwaltung des VIP-Systems und dürfen nicht manuell bearbeitet werden. Ausnahmen dazu sind in der nachfolgenden Tabelle aufgeführt; die Einstellungsmöglichkeiten sind in Kapitel 4 “Konfiguration” beschrieben.

  Zusätzlich enthält dieser Ordner noch weitere Unterverzeichnisse: **049** mit den deutschen Meldungen und Menüpunkten, **001** für die englische Version, **033** für französisch, **034** für spanisch, **039** für italienisch sowie die Verzeichnisse **filelist**, **log** und **viptools**.

  Die folgende Tabelle zeigt eine Übersicht über die Properties-Dateien mit einer Angabe, ob darin Änderungen vorgenommen werden dürfen oder nicht.

Tabelle 2 – Properties-Dateien von VIP

Dateiname	Manuelle Konfigurationen durch Administrator
addOns.properties	Nein
clientConfig.properties	Siehe “Voreinstellungen für Client-Installationen” auf Seite 58.
dbdefinition.properties	Nein
debug.properties	zur Fehlersuche
licence.properties	Nein
linux_editors.properties	Zur Voreinstellung von Bearbeitungs-programmen bei Client-Installationen, siehe “Vorgabe der Bearbeitungs-programme” auf Seite 55.
Message_{Ländercode}.properties	Nein
server.properties	Siehe “Wiederherstellen einer früheren Objektversion” auf Seite 59.
serverAddOns.properties	Nein
services.properties	Nein
sunos_i386_editors.properties	Siehe “Vorgabe der Bearbeitungs-programme” auf Seite 55.
sunos_sparc_editors.properties	Siehe “Vorgabe der Bearbeitungs-programme” auf Seite 55.
vipdbc.properties	Nein
websites.properties	Siehe “Datenbankanbindung” auf Seite 88.
windows_editors.properties	Siehe “Vorgabe der Bearbeitungs-programme” auf Seite 55.

- **debug:** Hier werden Debug-Informationen des Servers abgelegt, wenn dieser im Debug-Modus gestartet wird.
- **Export_Import:** Wird vom VIP-Server zur Zwischenablage von Objekten verwendet und dient zur Kommunikation zwischen den einzelnen VIP-Servern. Zusätzlich wird hier automatisch für jede Website ein Verzeichnis angelegt, dieses dient dem VIP-Server als temporäre Ablage.
- **Help:** Hier sind die Hilfedateien im HTML-Format abgelegt.
- **java:** Hier befinden sich die Java-Klassen des Servers und des Clients, die dann bei der Verbindung übertragen werden. Werden über das Server-API eigene Java-Klassen eingebunden, so sind diese in das Unterverzeichnis **\java\user** zu kopieren.
- **lib:** In diesem Verzeichnis sind die jar-Dateien enthalten.
- **MasterWebSite:** Enthält die Startseiten, die beim Anlegen einer Website benötigt werden.
- **ressource:** Quellen für die VIP-Clients.
- **website_1 ... website_n:** Hier sind die Objekte der einzelnen Websites enthalten. Das Einrichten und Verwalten von Websites wird über das Administrationssystem durchgeführt. Die Inhalte dieser Verzeichnisse sollen daher nicht manuell geändert werden. Die Benennung der Verzeichnisse entspricht den Namen der entsprechenden Websites.

Dateistruktur des Administrationsservers

Die Funktionalität und Struktur des Administrationsservers unterscheidet sich von allen anderen Servern. Der Administrationsserver dient zum Verwalten von Websites, Benutzern und Benutzergruppen. Daher enthält dieser Server keine eigenen Websites und Objekte. Unter **\admin\UserAdmin** befinden sich Konfigurationsdateien, in denen die Gruppen- und Benutzerinformationen sowie die Zuordnung zwischen Websites, Gruppen und Benutzern enthalten sind.

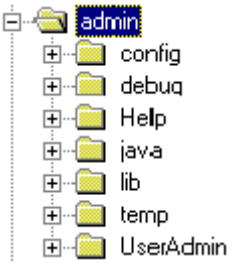

Abb. 5 – Die Struktur des Administrationsservers

Websites

Eine Website ist ein Menge von logisch verknüpften Objekten wie HTML-Seiten, GIF-Bildern usw. Alle Inhalte einer Website werden in Form von Dateien in Verzeichnissen abgelegt. Dies sind die Objekte, die mit dem VIP'ContentManager verwaltet werden.

Aufgrund des Multiserver-Konzepts werden die erstellten Websites eines VIP-Systems mehrfach abgelegt, nämlich auf dem Pflegeserver, dem QS-Server und dem Produktionsserver. Die Anzahl verschiedener Websites hängt von verschiedenen Überlegungen ab. Eventuell soll z. B. die Internet-Website getrennt vom firmeninternen Intranet verwaltet und publiziert werden. In der Praxis könnte auch die Aufteilung eines Intranets in mehrere Websites sinnvoll sein, um z. B. die Intranet-Seiten einzelner Abteilungen voneinander abzugrenzen.

Die einzelnen Websites enthalten die folgende Struktur:

Abb. 6 – Verzeichnisstruktur einer Website

- **Objekte:** Dient dem VIP-Server als Ablage für sämtliche freigegebene Objekte. Alte Versionen dieser Objekte werden dabei nicht überschrieben,

sondern in diesem Verzeichnis archiviert. Zusätzlich wird hier eine Kopie der Objekttabelle abgelegt.

- **Tables:** Enthält unter anderem die Systemtabellen der VIP-Server. Des weiteren werden in diesem Verzeichnis die Formattabellen der über VIP'DBC eingebundenen Tabellen abgelegt. Es bietet sich auch an, dort die Tabellen selbst abzulegen. Die CSV-Tabellen dieses Verzeichnisses, die mit der Grundkonfiguration ausgeliefert werden, sind u. a. folgende:
  - **format.csv**
  - **ID**
  - **ID.bak**
  - **labelList.properties**
  - **meta.csv**
  - **meta_fmt.csv**
  - **objekte.csv**
  - **objekte_filter_fmt.csv**
  - **objekte_fmt.csv**

  Hinweis: Die oben aufgeführten Tabellen dürfen weder gelöscht noch umbenannt werden.

- **Templates:** Dieses Verzeichnis enthält Vorlagen für Standardobjekte (HTML-Seiten, Themen, Grafiken usw.). Wenn ein Benutzer im Pflegesystem ein leeres Objekt anlegt (d. h. ohne Angabe einer Quelldatei für den Inhalt), wird der Inhalt aus dem entsprechenden Standardobjekt eingefügt.
- **WebSite:** Die Inhalte (Objekte) der Website befinden sich in diesem Verzeichnis. Sie sind jeweils in die Unterverzeichnisse der jeweiligen Themen und Unterthemen der Website unterteilt.

Themen und Unterthemen

Das VIP-System enthält ein separates Verzeichnis für jede Website. Insofern kann jede Website als ein abgeschlossenes Intranet betrachtet werden. Im Verzeichnis für jede Website befindet sich das Unterverzeichnis “WebSite”.

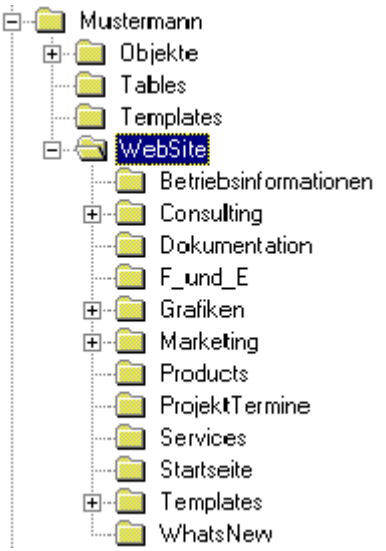

Abb. 7 – Inhalte befinden sich im Verzeichnis WebSite

Für jedes Thema einer Website wird ein eigenes Verzeichnis unterhalb des WebSite-Verzeichnisses angelegt, z. B. **\Mustermann\WebSite\Startseite**. Dies geschieht automatisch beim Erstellen eines Themas. Die Unterthemen befinden sich ebenfalls in separaten Verzeichnissen, die unter dem jeweiligen Themenverzeichnis angelegt werden.

Speicherung von Website-Objekten

Die Objekte einer Website werden in den WebSite-Verzeichnissen verwaltet.

- Die aktuellen Versionen aller in der Website enthaltenen Objekte werden im Verzeichnis **\WebSite** (z. B. **\Mustermann\WebSite**) bzw. in den darunter liegenden Themenverzeichnissen und -unterverzeichnissen gespeichert.
- Die jeweiligen Vorgängerversionen werden im Verzeichnis **\Objekte** (z. B. **\Mustermann\Objekte**) eingestellt.
- Ältere Versionen der Objekte werden im Backup-Verzeichnis (**\Edit\Backup**) abgelegt. Der Dateiname dieser Objekte ist folgendermaßen zusammengesetzt

  {website-name}_{objekt-ID}.{ext}.{version}

  (z. B. **\Edit\Backup\Mustermann_201.htm.0**).

  Hinweis: Die Dateien in den Verzeichnissen **\WebSite** und **\Objekte** werden zur Objektverwaltung benötigt und dürfen auf keinen Fall gelöscht oder direkt bearbeitet werden. Die im Verzeichnis **\Backup** gespeicherten Objekte werden vom VIP-System hingegen nicht mehr benötigt und können – gegebenenfalls – ausgelagert, archiviert oder auch gelöscht werden. Bitte beachten Sie jedoch, daß es nicht möglich ist, einen älteren Versionsstand eines Objekts zu rekonstruieren, wenn die Objektdaten aus dem Backup-Verzeichnis entfernt worden sind und nicht mehr zur Verfügung stehen.

KAPITEL 3
Installation

3.1 Voraussetzungen

Als Web Content Management System setzt der VIP'ContentManager einen Webserver und das Java-Development-Kit (JDK) als notwendige Komponenten voraus. Darüber hinaus wird ein Mailserver benötigt, um im Pflege-QS-Zyklus die automatische Benachrichtigung zwischen Pflege- und QS-System zu gewährleisten.

Bei der Installation des VIP'ContentManager handelt es sich ausschließlich um serverseitige Installationen und Komponenten, so daß keine Softwareverteilung notwendig ist. Für die Clients, also für die Arbeitsplätze der Webautoren und der Mitarbeiter der Qualitätssicherung, wird lediglich ein Webbrowser benötigt. Auf diesen Arbeitsplätzen muß freier Festplattenspeicher für die Zwischenablage von ausgeliehenen Objekten zur Verfügung stehen. Für die Bearbeitung von Objekten müssen auf den Arbeitsplätzen die entsprechenden Bearbeitungsprogramme (Grafikprogramme, HTML-Editoren usw.) installiert werden.

Erforderliche Komponenten

Java-Development-Kit (JDK)

Zum Ausführen der VIP-Serverprogramme wird das Java-Development-Kit (JDK) benötigt. Da alle VIP-Programme – einschließlich der Installationsroutinen – vollständig in Java implementiert sind, muß das JDK vor der Installation des VIP'ContentManager verfügbar sein.

Hinweis: Angaben zu den unterstützten Versionen des JDK sind in der Freigabemitteilung enthalten.

Webserver

Installieren Sie auf dem für das VIP-System gewählten Computer einen Webserver (z. B. Netscape Enterprise Server, Apache, Microsoft Internet Information Server).

Der Webserver muß entsprechend konfiguriert werden, um die von VIP verwalteten Informationen bereitstellen zu können. Lesen Sie die Informationen des jeweiligen Herstellers genau durch, und gehen Sie wie dort beschrieben vor.

Mailserver

Die Benachrichtigung von zuständigen Personen im VIP'ContentManager erfolgt per E-Mail. Daher muß ein Mail-Server installiert und konfiguriert sein. Der VIP'ContentManager nutzt zum Versenden von E-Mails das SMTP-Protokoll, das von den meisten Mail-Servern unterstützt wird oder über ein entsprechendes Gateway aktiviert werden kann.

Erweiterte Komponenten

Datenbankanbindung

Um eine Datenbankanbindung einzurichten, werden für die Grundinstallation von Java noch die JDBC-Klassen (Java Database Connectivity) benötigt. Die Umgebungsvariable CLASSPATH muß dementsprechend angepaßt werden. Darüber hinaus muß auf dem Server, auf dem VIP installiert ist, ein Datenbankzugriff über JDBC realisiert und eine Datenquelle eingerichtet sein.

Bei Windows NT- oder Solaris-Servern wird lediglich ein ODBC-Treiber benötigt. Dafür ist es jedoch notwendig, die JDBC-ODBC-Bridge zu installieren. Diese kann von der SUN-Website heruntergeladen werden (http://www.javasoft.com). Auch hier müssen die entsprechenden ODBC-Datenquellen eingerichtet werden.

Weitere Informationen zum Einrichten einer Datenbankanbindung finden Sie im Abschnitt 4.6 "Datenbankanbindung" auf Seite 88.

Firewalls

Wenn das VIP-System über mehrere Server verteilt ist, müssen bei vorhandenen Firewalls die entsprechenden Port-Adressen der VIP-Server freigeschaltet werden.

Serverseitige Anwendungen

In Verbindung mit dem VIP'ContentManager lassen sich sämtliche Möglichkeiten der Webtechnologie nutzen, zum Beispiel Java-Applets, CGI-Skripte, serverseitige Includes (SSI), Servlets usw. Teilweise werden hierfür serverseitige Installationen und/oder Konfigurationen benötigt, die allerdings nicht das VIP-System betreffen und daher keine Änderungen am VIP-System erfordern.

3.2 Installation der VIP-Server

Wichtige Hinweise zur Installation

Die Installation des VIP-Systems auf dem Server darf nicht unter dem Benutzernamen "Administrator" bzw. bei einem Unix-Server nicht unter dem Namen "root" erfolgen. Die Installation sollte unter einer eigenen Benutzergruppe (beispielsweise VIP_ADMIN) durchgeführt werden.

Unter Windows ist bei der Angabe des Zielpfades im Installationsprogramm bzw. bei der Anpassung von Verzeichnispfaden in der Datei **startvip.bat** auf die korrekte Groß-/Kleinschreibung der Verzeichnisnamen zu achten.

Installationsvorgang

Das Installationsprogramm wird bei Windows NT- und Unix-Servern unterschiedlich gestartet:

- **Windows NT:** Öffnen Sie die MS-DOS-Eingabeaufforderung, wechseln Sie auf das CD-ROM-Laufwerk, und rufen Sie das Installationsprogramm mit dem Pfad auf Ihr JDK-Verzeichnis als Parameter auf:

  install {JDK-Verzeichnispfad}\bin

- **Unix:** Auf der VIP-CD 1 “Versatile Installation Program” wird ein Jar-Archiv mitgeliefert, das Sie auf Ihren Server übertragen und in ein temporäres Verzeichnis entpacken müssen. Wechseln Sie in das entpackte Verzeichnis, und rufen Sie von dort aus das Installationsskript auf:

  sh ./install.sh

  Anschließend werden Sie aufgefordert, den Pfad auf Ihr JDK-Verzeichnis (**{JDK-Verzeichnispfad}/bin**) einzugeben.

Es erscheint der folgende Dialog, in dem verschiedene Einstellungen für die Installation festzulegen sind:

- die *Sprache* für den Installationsprozeß
- *Ihre Lizenzdatei:* Standardmäßig wird die VIP-Serverlizenz auf Diskette ausgeliefert. Legen Sie die Diskette ein, und geben Sie hier den Pfad auf Ihr Diskettenlaufwerk an, damit die VIP-Serverlizenz eingelesen werden kann.
- *Zielpfad:* Geben Sie den Pfad auf das gewünschte Installationsverzeichnis für das VIP-System an.

> **Hinweis:** Sie können im angegebenen Zielpfad beliebige Separatoren (“\” oder “/”) verwenden. Beachten Sie jedoch, daß der Pfad nicht mit einem Separator (“\” oder “/”) enden darf!

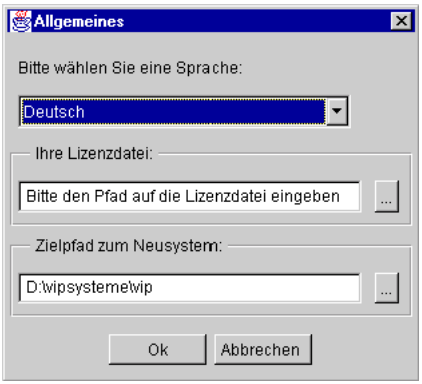

Abb. 8 – Allgemeine Einstellungen für die VIP-Installation

Nach dem Aufruf öffnet sich das Installationsfenster:

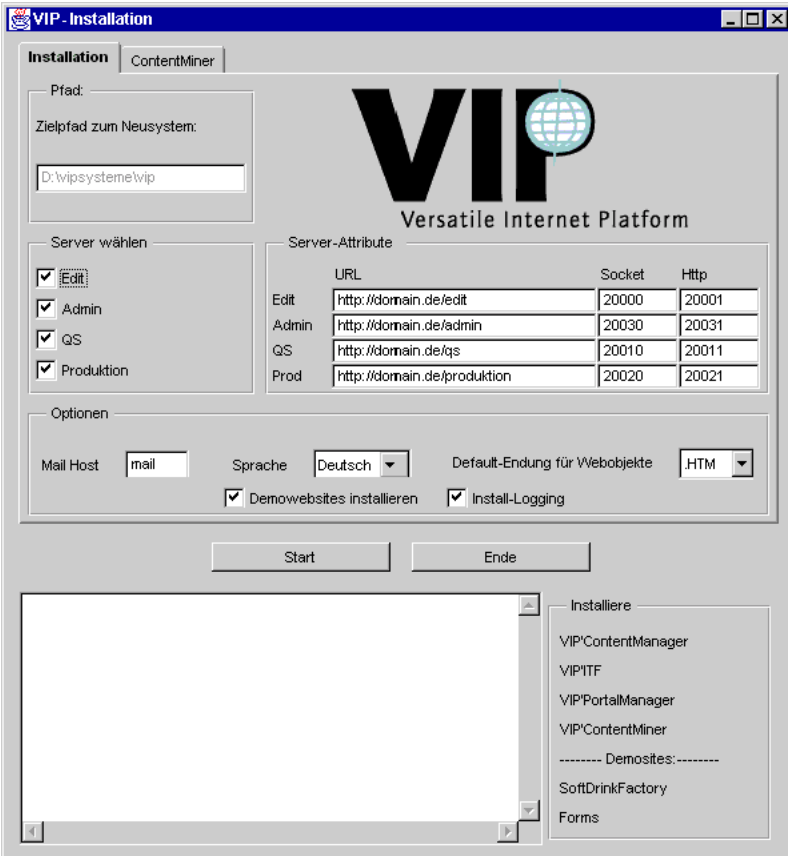

Abb. 9 – Installationseinstellungen

Die Eingabe- und Optionsfelder haben folgende Bedeutung:

Pfad

- *Zielpfad zum Neusystem:* Das Installationsverzeichnis für das VIP-System. Das Verzeichnis wird angelegt, wenn es noch nicht existiert.

Server wählen

- *Edit, Admin, QS, Produktion:* Mit diesen Optionsfeldern geben Sie an, welche VIP-Systeme Sie auf dem aktuellen Computer installieren möchten. Ein vollständiges VIP-System benötigt zwar alle vier VIP-Server, diese können jedoch auf unterschiedlichen Computern installiert werden. Dazu müssen Sie das Installationsprogramm auf dem jeweiligen Computer ausführen und den zu installierenden Server auswählen.

  Beispiel: Sie möchten Ihre Internet-Website mit dem VIP'ContentManager verwalten. Dazu wollen Sie die Pflege- und Qualitätssicherungssysteme auf einem internen Computer "Server A" ausführen. Das Prokuktionssystem soll sich auf einem Internet-Server "Server B" befinden. Führen Sie dann zunächst die Installation auf dem Computer "Server A" aus, und installieren Sie dort den Edit-, QS- und Administrationsserver und danach auf "Server B" den Produktionsserver. Natürlich müssen für jeden Server die im Abschnitt "Erforderliche Komponenten" auf Seite 31 genannten Komponenten verfügbar sein.

  Wichtige Anmerkung für verteilte Systeme: Damit bei verteilten Systemen die Kommunikation zwischen den einzelnen Servern gewährleistet werden kann, müssen die folgenden Eigenschaften für alle vier Server korrekt eingestellt werden. Dies ist notwendig, da die VIP-Systeme untereinander kommunizieren und somit jeder Kommunikationsteilnehmer über die anderen Systeme informiert sein muß.

Server-Attribute

- *URL:* Dies ist die HTTP-Adresse, unter der das jeweilige VIP-System zu erreichen ist. Die Adresse muß den Verzeichnisnamen des jeweiligen Systems beinhalten, also: http://{servername}/{system}.

  Tip: Nach dem Eintragen einer kompletten URL für den Edit-Server können Sie durch Betätigen der TAB-Taste bewirken, daß alle anderen URL-Felder der Serverinstallation mit entsprechenden Einträgen gefüllt werden.

- *Socket:* Dies ist die Port-Nummer, unter der dieser VIP-Server zum Aufbau einer Socket-Verbindung erreicht werden kann. Achten Sie darauf, daß die Port-Nummer nicht von anderen Anwendungen benutzt wird.
- *Http:* Hier wird die Port-Nummer eingegeben, über die eine HTTP-Verbindung (HTTP-Tunneling) ermöglicht wird. Achten Sie auch hier darauf, daß die Port-Nummer nicht von anderen Anwendungen verwendet wird. Sind zwischen den einzelnen Servern oder zwischen Client (Webautor, QS-Beauftragter) und Server Firewalls vorhanden, sind die entsprechenden Port-Adressen freizuschalten.

> **Wichtiger Hinweis:** Bitte beachten Sie, daß die eingegebenen Werte für die Port-Nummern *nicht* größer als 32000 sind. Wird ein größerer Wert eingegeben, ist der Einsatz der Zugriffsschutzkomponente (siehe Abschnitt 4.4 “Zugriffsschutz” auf Seite 60) nicht mehr möglich.

Optionen

- *Mail Host:* Geben Sie den Namen des Mailservers ein, unter dem dieser vom aktuellen Server aus angesprochen werden kann.
- *Sprache:* Wählen Sie die Standardsprache, in der das System installiert werden soll.
- *Default-Endung für Webobjekte:* Wählen Sie hier die Standard-Dateinamenerweiterung für Webobjekte aus.
- *Demowebsites installieren:* Wenn Sie eine Lizenz für den VIP’PortalManager besitzen, haben Sie mit dieser Option die Möglichkeit, die Demowebsites “SoftDrinkFactory” und “PressRelease” zu installieren.
- *Install-Logging:* Es wird nur dann ein Installationsprotokoll im Zielverzeichnis gespeichert, wenn diese Option vor dem Installationsvorgang aktiviert wurde.

> **Hinweis:** Nach der Installation einer Website ist dieser Website zunächst nur der Benutzer “admin” zugeordnet. Alle anderen Benutzer müssen der Website erst zugeordnet werden, bevor sie darauf zugreifen können. Weitere Informationen dazu finden Sie unter “Zuordnung von Benutzern zu einer Website” auf Seite 132.

Klicken Sie im Installationsdialog auf *Start*, um den Installationsvorgang zu starten.

Installationsprotokoll

Das Installationsprotokoll wird im Programmfenster angezeigt. Zusätzlich wird das Protokoll für jedes VIP' Produkt in folgende separate Datei geschrieben:
{VIP-Installationsverzeichnis}\installation\ install_{Produktname}_log.out

Eventuell auftretende Fehler werden jeweils in folgender Datei protokolliert:
{VIP-Installationsverzeichnis}\installation\ install_{Produktname}_err.out

Fehler, die schon ein Starten des Installationsprozesses verhindern, werden in diese Datei geschrieben:
{VIP-Installationsverzeichnis}\installation\InstallErr.out

Verteilte Installation

Der VIP'ContentManager ist ein Verbundsystem, bestehend aus den vier VIP-Servern *Edit*, *QS*, *Produktion* und *Administration*. Die VIP-Server können auf einem oder verschiedenen Computern installiert werden. In diesem Abschnitt werden die notwendigen Maßnahmen für eine Installation auf mehreren Rechnern erläutert.

Sicherheit durch Verteilung

Da der Zugang zum Produktionssystem einer breiteren Öffentlichkeit zur Verfügung gestellt werden soll als bei den drei anderen Systemen (Pflege-, QS- und Administrationssystem), kann es sinnvoll sein, das Produktionssystem separat von den anderen Systemen zu installieren. Dies trifft z. B. bei der Unterstützung von Intranet- und insbesondere Internet-Auftritten zu.

HTTP-Tunneling

Typischerweise werden Sicherheitsanforderungen bei der Verteilung der VIP-Systeme durch Firewall-Systeme gelöst. Firewall-Systeme interpretieren den Datenstrom und schalten u. a. nur bestimmte Protokolle frei. Der VIP'ContentManager berücksichtigt diese Tatsache, indem der Datentransfer

zwischen verschiedenen VIP-Systemen wahlweise im direkten Protokoll oder verpackt als HTTP-Datenstrom durchgeführt werden kann. Dieses ist ein übliches Verfahren, das als “Tunneling” bekannt ist (in diesem Fall “HTTP-Tunneling”).

Wenn Sie planen, VIP-Systeme über Firewalls hinweg zu verbinden, muß eine HTTP-Verbindung freigeschaltet werden. Dieses ist im Firewall-System entsprechend zu konfigurieren.

HTTP-Tunneling wird von jedem VIP-Server unterstützt; es beschränkt sich also nicht auf die Verbindung zwischen Qualitätssicherungs- und Produktionssystem.

Lastverteilung

Neben einer verteilten Installation aus Gründen der Zugangssicherheit kann die Installation auf verschiedene Computer verteilt werden, um eine Lastverteilung zu erreichen. Dabei treten jedoch potentiell Performance-Verluste (zumindest bei Massenoperationen) auf, denn bei einer verteilten Installation muß der Austausch von Web-Objekten zwischen den VIP-Systemen über die Netzverbindung erfolgen. Bei einer Installation aller VIP-Server auf einem einzigen Computer findet der Austausch von Web-Objekten dagegen lokal im Dateisystem statt.

Meistens sind die Nachteile durch den Dateitransfer über das Netzwerk geringer als die durch eine Lastverteilung entstehenden Vorteile. Ausschlaggebend ist dabei die Geschwindigkeit des Netzwerks.

Auswirkungen auf sekundäre Systeme

Eine Verteilung hat keine Auswirkungen auf die von Ihnen mit dem VIP'Content-Manager verwalteten Websites, da diese grundsätzlich zwischen den Systemen getrennt werden.

Beachten Sie aber, daß bei einer Verteilung Ihres VIP-Gesamtsystems gegebenenfalls andere Subsysteme mehrfach vorhanden sein müssen. Wenn Sie beispielsweise eine datenbankgestützte Speicherung der Objekttabellen und Metadaten eingerichtet haben, müssen Sie das Datenbanksystem unter Umständen mehrfach (auf jedem Server-Computer) installieren.

Dasselbe trifft auch für Ihre Web-Server zu: Bedenken Sie, daß die VIP-Server einen Web-Server (HTTP-Server) zur Publikation der Web-Objekte benötigen. Wenn Sie eine Verteilung der VIP-Systeme anstreben, müssen Sie auch Web-

Server auf allen Server-Computern installieren. Der VIP'ContentManager unterstützt verschiedene Web-Server. Bei einer Verteilung der VIP-Server können auf den Server-Computern verschiedene Web-Server zum Einsatz kommen.

Ebenso müssen Sie größeren Aufwand betreiben, wenn Sie VIP-Server-Agenten so schreiben, daß Agenten zwischen zwei VIP-Systemen in Verbindung stehen. Dies ist häufig der Fall, wenn ein paralleler Work- oder Informationsflow durch Agenten implementiert ist. Bei einer Verteilung müssen die Agenten in der Lage sein, verteilt zu operieren.

Verbindungen zwischen den Servern

Die folgende Abbildung zeigt, welche Verbindungen zwischen den VIP-Servern benötigt werden. Die Kommunikation zwischen VIP-Servern läuft jeweils über denselben Port. So benutzt beispielsweise das Editsystem denselben Port am Admin-Server wie das Qualitätssicherungssystem, und alle VIP-Clients nutzen denselben Port zum Qualitätssicherungssystem bzw. zum Pflegesystem.

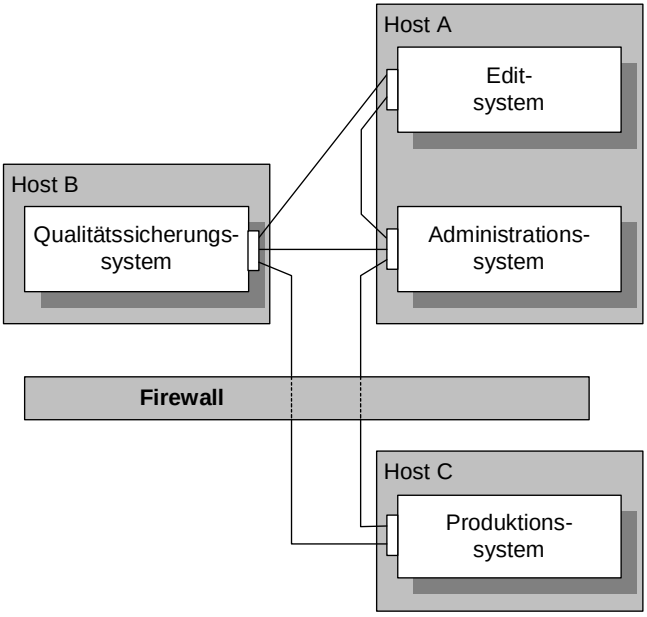

Abb. 10 – Beispiel einer verteilten Installation auf mehreren Server-Computern (Hosts)

Ein VIP-Server belegt grundsätzlich zwei Ports, von denen jedoch meistens nur einer benutzt wird. Der erste Port ist der für direkte Kommunikation. Beim Verbindungsaufbau wird zuerst versucht, die Verbindung über diesen Port herzustellen. Schlägt der Verbindungsaufbau fehl (etwa weil ein vorgeschaltetes Firewall-System die Verbindung ablehnt), wird versucht, die Verbindung über den zweiten Port aufzubauen. Dieser Port verwendet HTTP-Tunneling zur Datenübertragung.

Installationsvorgang

Die Installation eines verteilten VIP-Systems unterscheidet sich nur geringfügig von der Installation eines lokalen Systems. Bevor Sie beginnen, sollten Sie pro VIP-Server zwei freie Ports bestimmen. Wenn Sie also die Installation aller vier VIP-Server auf einem Server-Computer vornehmen, benötigen Sie acht freie Ports. In den meisten Fällen können die bei der Installation vorgegebenen Standardwerte übernommen werden.

Die Installation eines verteilten VIP-Systems wird über den gewohnten Installationsvorgang durchgeführt, es muß aber auf jedem Server-Computer eine separate Installation vorgenommen werden.

Hinweise:

Achten Sie bei der Installation der einzelnen VIP-Server darauf, daß Sie **nur** den gewünschten Server-Typ markiert lassen. Standardmäßig sind im Installationsfenster immer alle vier VIP-Server markiert.

Auch wenn Sie nicht alle vier VIP-Server auf einem Computer installieren, müssen Sie immer **alle** URLs und Ports der VIP-Server angeben. Orientieren Sie sich dabei an den vorgegebenen Standardwerten, und ändern Sie die Host-Namen (Computer-Namen) und die Port-Nummern entsprechend.

Beispiel 1

Sie planen, das Edit- und das Administrationssystem auf einem Computer zu installieren (“hostA”), das Qualitätssicherungssystem auf einem zweiten (“hostB”) und das Produktionssystem auf einem dritten (“hostC”). Das Produktionssystem ist durch ein Firewall-System von den anderen Systemen abgeschottet (siehe

Abbildung 10 “Beispiel einer verteilten Installation auf mehreren Server-Computern (Hosts)” auf Seite 40).

Um diese Beispielkonstellation zu realisieren, gehen Sie wie folgt vor:

1. Installieren Sie Ihre Webserver auf allen drei Server-Rechnern. In diesem Beispiel sollen die Webserver ihren Service unter folgenden URLs anbieten: **hostA.domain.de**, **hostB.domain.de** und **hostC.domain.de**. (Anstelle des Platzhalters **domain.de** verwenden Sie natürlich die tatsächliche Bezeichnung Ihrer Domain).
2. Installieren Sie auf dem Computer “hostA” das Edit- und Administrationssystem, indem Sie diese beiden Server-Typen auswählen. Geben Sie dort folgende URLs und Ports an (als Ports dürfen Sie auch andere freie Ports wählen):

	URL	Socket	HTTP
Edit:	http://hostA.domain.de/edit	20000	20001
Admin:	http://hostA.domain.de/admin	20030	20031
QS:	http://hostB.domain.de/qs	20010	20011
Prod:	http://hostC.domain.de/produktion	20020	20021

3. Installieren Sie auf dem Computer “hostB” das Qualitätssicherungssystem, indem Sie nur diesen Server-Typ auswählen. Geben Sie **dieselben** URLs und Ports wie für “hostA” an!
4. Installieren Sie auf dem Computer “hostC” das Produktionssystem, indem Sie nur diesen Server-Typ auswählen. Wählen Sie auch hier dieselben URLs und Ports.
5. Konfigurieren Sie das Firewall-System so, daß der HTTP-Port zum Produktionssystem in die eine Richtung freigeschaltet wird (im Beispiel: Port 20021) und der HTTP-Port vom Produktions- zum Administrationssystem in die andere Richtung.

Steuerung der Installation

Aufruf

Die Standardinstallation wird über den Install-Batch aufgerufen. In dieser Datei wird das Programm **Installation.class** im Package **de.gauss.vip98.installation** im Archiv **installation.jar** aufgerufen.

Der Aufruf des Install-Batch muß mit der Angabe des JDK-Pfades erfolgen. Im folgenden Beispiel ist ein möglicher Aufruf dargestellt.

```
install d:\jdk1.1.8\bin
```

Nach erfolgter Eingabe wird die grafische Oberfläche der Installation aufgerufen.

Steuerung durch Aufrufparameter

Durch den Aufrufmodus und die Aufrufparameter kann das Verhalten des Installationsprogramms gesteuert werden.

Es gibt zwei Varianten des Aufrufs:

- Installation über die grafische Oberfläche
- Offline-Installation

Installation über die grafische Oberfläche

Die Installation über die grafische Oberfläche erfordert nur die Angabe des JDK-Parameters (siehe oben).

Offline-Installation

Die Offline-Installation wird durch den Aufruf der VIP-Installationsklasse mit dem Parameter `-N` gestartet. Der Aufruf könnte wie im folgenden Beispiel aussehen:

```
java -classpath .\java;java\installation.jar;java\vipserver.jar; ➪
  lib\collection.jar de.gauss.vip98.installation.Installation ➪
    -JDK d:\jdk1.1.8\bin -N -M c:\temp\install.properties
```

Die einzelnen Parameter haben folgende Bedeutung:

`-JDK`	Angabe des JDK-Pfades ist erforderlich
`-?`	Aufruf der Hilfe
`-M`	Angabe der Master-Command-Datei
`-N`	Offline-Installation
`classpath`	Klassenpfad auf die VIP-Installationsklassen. Dieser Parameter soll so gesetzt sein wie in der Datei **install.bat** (bzw. **install.sh**).

Wird der Parameter `-M` nicht angegeben, wird die Datei **install.properties** aus dem aktuellen Verzeichnis, aus dem die Installation aufgerufen wurde, verwendet.

Auch bei der Offline-Installation werden die im Abschnitt “Installationsprotokoll” auf Seite 38 beschriebenen Protokolle geschrieben. Wenn die Offline-Installation nicht gestartet werden kann, wird der Fehler in der Datei **{VIP-Installationsverzeichnis}\installation\InstallErr.out** protokolliert.

Die Master-Command-Datei install.properties

Für die Offline-Installation müssen in der Datei **install.properties** die erforderlichen Angaben gemacht werden. Diese werden im folgenden beispielhaft dargestellt:

```
# General data
LICENSEDIR=c:|temp|
JDK_PATH=d:|jdk1.1.8.|bin|
INSTALL_DIR=c:|vip5e|
MAILHOST=mail
LANGUAGE=049
WEBOBJECT_DEFAULT_SUFFIX=.htm
LOGGING=YES

# Install servers
EDIT=YES
ADMIN=YES
QA=YES
PRODUCTION=YES

# Data of edit-server
EDIT_ADDRESS=http://vipserver.mustermann.de/vipsysteme/edit
```

```
EDIT_SOCKET=20000
EDIT_HTTP=20001

# Data of admin-server
ADMIN_ADDRESS=http://vipserver.mustermann.de/vipsysteme/admin
ADMIN_SOCKET=20030
ADMIN_HTTP=20031

# Data of qa-server
QA_ADDRESS=http://vipserver.mustermann.de/vipsysteme/qs
QA_SOCKET=20010
QA_HTTP=20011

# Data of prod-server
PROD_ADDRESS=http://vipserver.mustermann.de/vipsysteme/produktion
PROD_SOCKET=20020
PROD_HTTP=20021
```

Wenn Sie zusätzlich eine Lizenz für den VIP’ContentMiner erworben haben und die Demo-Websites für den VIP’PortalManager installieren möchten, müssen Sie die folgenden Einträge hinzufügen:

```
# Activate ContentMiner
ACTIVATE_COMI_FOR_EDIT=YES
ACTIVATE_COMI_FOR_QA=NO
ACTIVATE_COMI_FOR_PROD=YES
COMI_INDEX_PORT=9000
COMI_QUERY_PORT=9001

# Install demosites
[SOFTDRINKFACTORY]
[PRESSRELEASE]
```

Pfadangaben

LICENSEDIR

Das Verzeichnis, in dem sich die Lizenz befindet.

JDK_PATH

Der Pfad auf das JDK-Verzeichnis.

INSTALL_DIR

Das Zielverzeichnis, in welches das VIP-System installiert werden soll.

Auswahl der zu installierenden Server

EDIT=YES | NO

ADMIN=YES | NO

QA=YES | NO

PRODUCTION=YES | NO

Durch die Angabe von YES bzw. NO wird festgelegt, ob die einzelnen Server installiert werden sollen oder nicht.

Server-Attribute

EDIT_ADDRESS

Die HTTP-Adresse, unter der der Edit-Server zu erreichen ist.

EDIT_SOCKET

Die Port-Nummer, unter der der Edit-Server zu erreichen ist.

EDIT_HTTP

Die Port-Nummer, über die eine HTTP-Verbindung (HTTP-Tunneling) zu dem Edit-Server ermöglicht wird.

ADMIN_ADDRESS

Die HTTP-Adresse, unter der der Admin-Server zu erreichen ist.

ADMIN_SOCKET

Die Port-Nummer, unter der der Admin-Server zu erreichen ist.

ADMIN_HTTP

Die Port-Nummer, über die eine HTTP-Verbindung (HTTP-Tunneling) zu dem Admin-Server ermöglicht wird.

QA_ADDRESS

Die HTTP-Adresse, unter der der QA-Server zu erreichen ist.

QA_SOCKET

Die Port-Nummer, unter der der QA-Server zu erreichen ist.

QA_HTTP

Die Port-Nummer, über die eine HTTP-Verbindung (HTTP-Tunneling) zu dem QA-Server ermöglicht wird.

PROD_ADDRESS

Die HTTP-Adresse, unter der der Produktions-Server zu erreichen ist.

PROD_SOCKET

Die Port-Nummer, unter der der Produktions-Server zu erreichen ist.

PROD_HTTP

Die Port-Nummer, über die eine HTTP-Verbindung (HTTP-Tunneling) zu dem Produktions-Server ermöglicht wird.

Optionen

MAILHOST

Der Hostname, unter dem der Mailserver vom aktuellen Server aus angesprochen werden kann.

LANGUAGE

Die Standardsprache, in der das System installiert werden soll. Geben Sie dazu die internationale Telefonvorwahlnummer des Landes ein, in dessen Sprache Sie die Installation vornehmen möchten (049 für deutsch, 001 für US-amerikanisch, 033 für französisch).

WEBOBJECT_DEFAULT_SUFFIX=.htm | .html

Durch diese Angabe können Sie festlegen, ob .htm oder .html als Standard-Dateinamenerweiterung für Webobjekte verwendet wird.

LOGGING=YES | NO

Die Angabe von YES bzw. NO definiert, ob ein Installationsprotokoll im Zielverzeichnis gespeichert wird oder nicht.

ACTIVATE_COMI_FOR_EDIT=YES | NO

ACTIVATE_COMI_FOR_QA=YES | NO

ACTIVATE_COMI_FOR_PROD=YES | NO

Wenn Sie eine Lizenz für den VIP'ContentMiner besitzen, können Sie durch den entsprechenden Aufruf den VIP'ContentMiner für das jeweilige VIP-System aktivieren. Voraussetzung ist, daß der entsprechende Server auch installiert wird (Server=YES, siehe oben).

COMI_INDEX_PORT

Die Port-Nummer, auf die der Index-Server konfiguriert werden soll.

COMI_QUERY_PORT

Die Port-Nummer, auf die der Query-Server konfiguriert werden soll.

[SOFTDRINKFACTORY]

Wenn Sie eine Lizenz für den VIP'PortalManager besitzen, haben Sie zusätzlich die Möglichkeit, die Demo-Websites "SoftDrinkFactory" und "PressRelease" zu installieren.

[NO_SOFTDRINKFACTORY_UPDATE]

Wenn Sie ein Update auf eine neue Version durchführen, werden standardmäßig die bereits installierten Demowebsites aktualisiert. Generell wird die Verwendung der aktuellen Demowebsites empfohlen. Wenn Sie jedoch Änderungen an Ihren Demowebsites vorgenommen haben und sie aus diesem Grund nicht überschreiben möchten, ist diese Angabe vorzunehmen.

Installation der VIP-Serverlizenz

Durch die installierte Lizenz werden verschiedene Leistungseigenschaften des VIP-Systems gesteuert, z. B.:

- die maximale Anzahl von Benutzern, Websites und Objekten
- die Gültigkeitsdauer der Lizenz

In der Lizenz werden außerdem die Server (durch IP-Adresse) spezifiziert, auf denen die VIP-Systeme laufen sollen. Bei einer Demoversion bzw. Testinstallation sind diese Serverspezifikationen jedoch nicht enthalten.

Die VIP-Serverlizenz wird durch zwei Lizenzdateien gesteuert:

- **server.license** und
- **server.signature**.

Normalerweise wird die VIP-Serverlizenz automatisch während des eigentlichen Installationsprozesses auf dem Administrationsserver installiert (siehe “Installationsvorgang” auf Seite 33). Wenn Sie allerdings ein Update von einer Demoversion bzw. Testinstallation durchführen, sind beide Lizenzdateien in das **config**-Verzeichnis des Administrationssystems zu kopieren:

{VIP-Installationsverzeichnis}\admin\config

> **Hinweis:** Die Lizenzdateien werden getrennt von den Produkt-CDs ausgeliefert (standardmäßig auf einer Diskette). Nach Ablauf der Lizenzgültigkeit (etwa bei einer Demoversion) kann die Serverfunktionalität durch Installation neuer Lizenzdateien wiederhergestellt werden.

3.3 Starten der VIP-Server

Die VIP-Server müssen nur einmal gestartet werden und sollten danach ständig in Betrieb sein. Es bietet sich an, diese als Hintergrundprozesse auszuführen. Wichtig ist dabei, daß der Benutzer, unter dessen Namen diese Prozesse gestartet werden, über die erforderlichen Schreib- und Leseberechtigungen in den entsprechenden VIP-Verzeichnissen verfügen muß. Außerdem muß bei einer Datenbankanbindung die entsprechende Datenquelle auch für diesen Benutzer eingerichtet sein.

Achtung: Die VIP-Server dürfen nur unter dem Benutzernamen gestartet werden, unter dem sie installiert wurden. Auf keinen Fall dürfen die VIP-Server unter dem Administrator-Account gestartet werden!

Die VIP-Server werden auf NT- und Unix-Servern unterschiedlich gestartet:

- **Windows NT:** Öffnen Sie (z. B. im Windows Explorer) das Zielverzeichnis der Installation und führen Sie die Batch-Datei **`startvip.bat`** aus.
- **Unix:** Wechseln Sie in das Zielverzeichnis der Installation, und rufen Sie von dort aus das Startskript auf: **`sh ./start.sh`**.

Hinweis: Bei großen Websites empfiehlt es sich, die maximale Speichermenge heraufzusetzen, was eine Änderung in der jeweiligen Startdatei erfordert. Weitere Informationen finden Sie im Abschnitt 4.10 “Einstellen der Hauptspeicheranforderung” auf Seite 121.

3.4 Migration von VIP 3.0 auf VIP 5e

Arbeiten mit dem Offline-Werkzeug “AdjustURL”

Mit dem Offline-Werkzeug “AdjustURL” haben Sie die Möglichkeit, alle in einem VIP-System enthaltenen URLs in einem einzigen Migrationsvorgang an die neue standard-konforme Schreibweise gemäß dem Standard RFC 2396 anzupassen. Gehen Sie dazu folgendermaßen vor:

1. Bevor Sie die URL-Migration ausführen, müssen Sie die VIP-Server herunterfahren. Außerdem sollten Sie eine Sicherheitskopie von Ihren Daten anlegen.
2. Die Umgebungsvariable PATH muß den Pfad auf das Verzeichnis **{jdk-pfad}/bin** enthalten. Fügen Sie diesen notfalls hinzu.
3. Starten Sie eine Command-Shell / Eingabeaufforderung.
4. Setzen Sie die Umgebungsvariable CLASSPATH auf die Datei **{vipserver}/java/vipserver.jar**.
5. Wechseln Sie in das Basisverzeichnis von VIP, und rufen Sie von dort aus das Migrationswerkzeug auf. Führen Sie die im folgenden beschriebenen drei Aufrufe nacheinander aus:

Ersetzung prüfen

Im ersten Schritt wird das Ersetzungstool mit Ausgabe eines ausführlichen Protokolls (Verbose) im Testmodus ausgeführt. Anhand des Protokolls kann geprüft werden, ob die vorgenommenen Ersetzungen korrekt sind. Diesen Modus startet man mit dem folgenden Aufruf:

```
java -mx128M de.gauss.io.AdjustURL -u {url} -v {file}
```

`-v` (Verbose): Mit diesem Aufruf wird eine Ausgabedatei erzeugt, in der alle von der Ersetzung betroffenen Dateien und alle durchzuführenden Ersetzungen angegeben sind. Mit dem Parameter `{url}` wird die URL angegeben, die als Suchmuster für die Ersetzung verwendet werden soll. Hierbei sollte es sich normalerweise um das VIP-Basisverzeichnis handeln. Das Ergebnis wird in die mit `{file}` angegebene Datei geschrieben. Wenn dieser Parameter fehlt, wird die Ausgabe auf Standard-out geschrieben (dies ist die Default-Einstellung).

Ersetzungsliste erzeugen

Im zweiten Schritt wird das Ersetzungstool im “Generate”-Modus ausgeführt. Es wird – wie im “Verbose”-Modus – eine Liste der von der Ersetzung betroffenen Dateien erzeugt, jedoch ohne Angabe der einzelnen Ersetzungen. Anhand dieser Liste wird die eigentliche Ersetzung im dritten Schritt durchgeführt. Der “Generate”-Modus wird mit folgendem Aufruf gestartet:

```
java -mx128M de.gauss.io.AdjustURL -u {url} -g {file}
```

`-g` (Generate): Mit diesem Aufruf wird eine Ausgabedatei mit Angabe aller zu bearbeitenden Dateien erzeugt. Mit dem Parameter `{url}` wird die URL angegeben, die als Suchmuster für die Ersetzung verwendet werden soll. Dies soll normalerweise die Basis-URL des VIP-Systems sein. Das Ergebnis wird in die mit `{file}` angegebene Datei geschrieben. Beachten Sie bitte, daß in diesem Modus auf die Spezifikation einer Ausgabedatei nicht verzichtet werden kann, da es ansonsten keine Grundlage für den letzten Schritt geben würde.

Ersetzung durchführen

In diesem Schritt wird die Ersetzung durchgeführt, die mit folgendem Aufruf gestartet wird:

```
java -mx128M de.gauss.io.AdjustURL -u {url} -f {file}
```

`-f` (Force): Mit diesem Aufruf werden die URLs tatsächlich ersetzt, und zwar in allen in der generierten Ersetzungsdatei (siehe oben) aufgeführten Dateien. Mit dem Parameter `{file}` wird in diesem Fall die durch den zweiten Aufruf (Generate) generierte Ersetzungsliste als Eingabedatei spezifiziert. Eine Ausgabedatei gibt es bei diesem Aufruf nicht. Auch hier wird mit dem Parameter `{url}` die URL angegeben, die als Suchmuster für die Ersetzung verwendet werden soll.

KAPITEL 4
Konfiguration

4.1 Globale Arbeitsplatz-Voreinstellungen

Durch die Konfiguration des Pflegesystems können den Webautoren gewisse Vorgaben gemacht werden, die ihnen die Arbeit erleichtern. Dies betrifft die Wahl der Editoren und das VIP-Ablageverzeichnis auf den Autoren-Arbeitsplätzen.

Die Dateien, in denen Sie diese Konfigurationen vornehmen können, finden Sie im folgenden Konfigurationsverzeichnis:

{VIP-Installationsverzeichnis}\edit\config

Im folgenden Abschnitt wird beschrieben, um welche Dateien es sich dabei handelt.

> **Hinweis:** An anderen Dateien sollten Sie keine Änderungen vornehmen, da dies zu unerwünschten Ergebnissen führen kann.

Vorgabe der Bearbeitungsprogramme

In den Konfigurationsdateien **windows_editors.properties**, **linux_editors.properties** usw. (siehe unten) können Sie voreinstellen, in welchen Editoren die verschiedenen Objekttypen beim Ausleihen geöffnet werden. Dazu werden Dateiendungen mit den Installationspfaden der Editoren auf den Autorenarbeitsplätzen verknüpft. Sie können außerdem durch Angabe eines Parameters für jeden Editor festlegen, ob beim Öffnen einer Datei im Editor die nach RFC 2396 maskierten Sonderzeichen in URLs wieder zurück in Sonderzeichen umgewandelt werden. Dies kann in seltenen Fällen erforderlich sein, wenn ein Editor die beim Maskieren in die URLs eingesetzten Prozentzeichen falsch interpretiert.

Die Einträge in den Dateien sind lediglich Vorgaben. Jeder Benutzer kann diese Einstellungen im Hauptfenster des VIP'ContentManager im Menü *Extras* → *Optionen* ändern und eigene Bearbeitungsprogramme wählen. Weitere Informationen dazu finden Sie im Benutzerhandbuch.

Wenn für einen Objekt- bzw. Dateityp noch kein entsprechender Editor gewählt wurde oder das eingestellte Programm nicht verfügbar ist, wird der Benutzer aufgefordert, ein Programm festzulegen.

Für jedes Client-System gibt es eine entsprechende Konfigurationsdatei. Die Einstellungen werden folgendermaßen vorgenommen:

Windows

Die Einstellungen für die Vorgabe von Bearbeitungsprogrammen für Client-Systeme unter Windows stehen in der Datei **windows_editors.properties**. Die Einträge in dieser Datei haben folgende Syntax:

```
{Erweiterung}={Pfad}\{Anwendungsprogramm};{Beschreibung};{Parameter};⇨
  {0|1}
```

Der Parameter 0 bzw. 1 drückt aus, ob Ihr ausgewählter HTML-Editor URLs gemäß dem Standard RFC 2396 interpretiert.

- 0 = Die Option *URLs entsprechen RFC 2396* im Dialog *Dateitypen* ist deaktiviert.
- 1 = Die Option *URLs entsprechen RFC 2396* im Dialog *Dateitypen* ist aktiviert.

Die Datei **windows_editors.properties** könnte z. B. so aussehen:

```
DOC=C:\Programme\MSOffice\Winword\winword.exe;Winword-Datei;
HTM=C:\Programme\FrontPage\bin\fpeditor.exe;HTML-Datei; ;0
HTML=C:\Programme\FrontPage\bin\fpeditor.exe;HTML-Datei; ;0
TXT=C:\Programme\WindowsNT\Zubehör\Wordpad.exe;Text-Datei;
```

Unix

Für die verschiedenen Unix-Plattformen gibt es unterschiedliche Konfigurationsdateien, um die Bearbeitungsprogramme einzustellen. Diese heißen **sunos_i386_editors.properties**, **sunos_sparc_editors.properties** und **linux_editors.properties**.

Die Einstellungen in diesen Dateien ähneln den entsprechenden Windows-Einträgen:

```
{Erweiterung}={Pfad}/{Anwendungsprogramm}:{Beschreibung}:➪
  {Parameter}:{0|1}
```

Die Datei **linux_editors.properties** könnte z. B. so aussehen:

```
HTM=/usr/bin/netscape4.06/netscape:Web-Datei:-edit:0
HTML=/opt/netscape/netscape:Web-Datei:-edit:0
```

Als Optionen werden die Attribute angegeben, die das Anwendungsprogramm u. U. benötigt. Pfadangaben beziehen sich auf die Autorenarbeitsplätze.

Es kann vorkommen, daß Sie eine Dateiendung mit mehreren Anwendungen verknüpfen wollen, weil diese Anwendung auf den Autorenarbeitsplätzen an unterschiedlichen Stellen installiert ist, oder weil die einzelnen Autoren unterschiedliche Bearbeitungsprogramme benutzen. Sie können in den oben genannten Konfigurationsdateien einen Dateityp auch mehrmals angeben. Der VIP'ContentManager versucht dann, die entsprechende Anwendung in der Reihenfolge der Einträge zu starten und benutzt die erste, die sich starten läßt.

Änderungen in diesen Konfigurationsdateien können im laufenden Betrieb vorgenommen werden und sind danach sofort verfügbar.

Voreinstellungen für Client-Installationen

Für die lokale Installation des VIP'ContentManager und die Zwischenablage von ausgeliehenen Objekten wird auf jedem Client-Arbeitsplatz Festplattenspeicher benötigt. Die Voreinstellung für das lokale Installationsverzeichnis wird in der Datei **clientConfig.properties** auf dem Server festgelegt.

Die entsprechenden Einstellungen haben folgendes Format:

```
[windows]
# Pfad für VIP auf den Clients
CLIENTPATH=d:\\vip

[sunos_sparc]
# Pfad für VIP auf den Clients
CLIENTPATH=$HOME/vip

[sunos_i386]
# Pfad für VIP auf den Clients
CLIENTPATH=$HOME/vip

[linux]
# Pfad für VIP auf den Clients
CLIENTPATH=$HOME/vip
```

Bei der Angabe des Installationsverzeichnisses können Umgebungsvariablen verwendet werden. Dazu wird unter Unix der Variablenname mit einem vorausgehenden Dollarzeichen ($) eingesetzt, z. B. `$HOME`. Unter Windows wird der Variablenname zwischen Prozentzeichen (%) gesetzt, z. B. `%TEMP%`.

Beachten Sie bitte auch, daß der Backslash (\) in diesen Pfadangaben immer doppelt gesetzt werden muß, z. B. unter Windows: `CLIENTPATH=d:\\vip`.

4.2 Konfiguration des Webservers

Der VIP'ContentManager arbeitet mit allen gängigen Webservern zusammen, z. B. Apache, MS IIS, Netscape Enterprise Server. Die Konfiguration hängt vom verwendeten Webserver und dem Betriebssystem ab.

> **Hinweis:** Angaben zu den Versionsnummern der getesteten Webserver, die mit dem VIP'ContentManager zusammenarbeiten, finden Sie in der Freigabemitteilung. Wir bitten um Ihr Verständnis, daß wir an dieser Stelle nicht auf alle Konfigurationsmöglichkeiten eingehen können.

4.3 Wiederherstellen einer früheren Objektversion

Mit dieser Funktion können standardmäßig die letzten fünf Versionen eines Objekts wiederhergestellt werden. Eine abweichende Anzahl können Sie durch Hinzufügen des Eintrags `MAX_VERSION` in der Datei **`server.properties`** des Edit-Systems festlegen.

```
...
MAX_VERSION=10
```

> **Hinweise:**
>
> Bevor Sie den Eintrag in der Datei **`server.properties`** vornehmen, sollten Sie vorauschauend überlegen, wie viele Versionen Sie eventuell wiederherstellen möchten. Eine spätere Änderung der Anzahl wirkt sich nicht auf bestehende, sondern lediglich auf neu angelegte Objekte aus.
>
> Bitte beachten Sie, daß der Zugriff auf die Dateien umso langsamer wird, je größer der hier angegebene Wert ist.

4.4 Zugriffsschutz

Die Zugriffsschutzkomponente des VIP'ContentManager bietet die Möglichkeit, die Zugriffskontrolle aus dem Pflege- und Qualitätssicherungssystem (siehe Kapitel 6 "Zugriffskontrolle") auf das Produktionssystem zu übertragen. Damit ist im Produktionsbetrieb (also auch im Internet) eine objektspezifische Zugriffskontrolle auf alle Objekte einer Website möglich.

Hinweis: Angaben zu den unterstützten Systemen bzw. Plattformen sind in der Freigabemitteilung enthalten.

Funktionsweise

Die Zugriffsschutzkomponente ist als DLL (bzw. unter Unix als "Shared Library") implementiert. Diese wird in den Webserver eingebunden und sorgt dafür, daß alle Anfragen an den Webserver dahingehend geprüft werden, ob für die angeforderte Seite eine Zugriffsberechtigung erforderlich ist. Wenn ja, muß sich der Benutzer durch eine Anmeldung für den Zugriff auf die Seite authentifizieren.

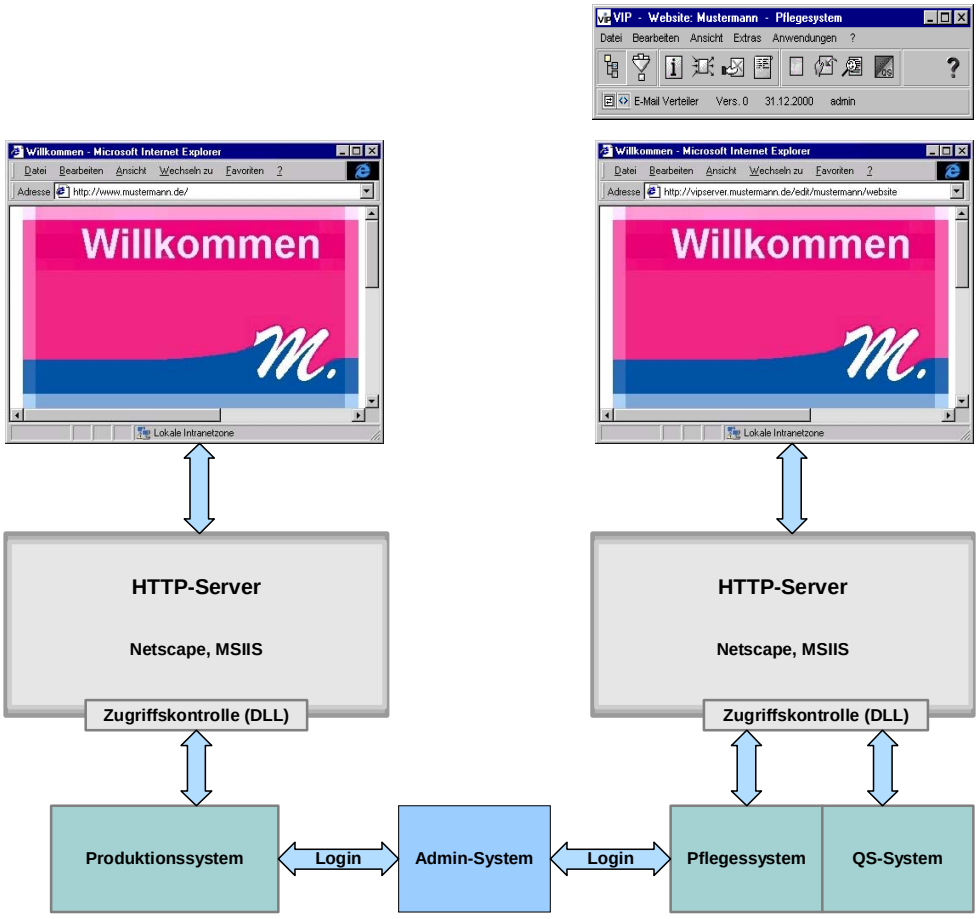

Abb. 11 – Zugriffsschutzkomponente im Überblick

Die Zugriffsschutzkomponente (DLL bzw. Shared Library) ist eine Art Filter, der beim Start des Webservers mit eingebunden wird. Jede Anfrage an den Webserver läuft über diesen Filter, der die Zugriffsberechtigung für das angeforderte Objekt überprüft.

Der Benutzer stellt eine Anfrage (Request) an den Webserver. Dieser empfängt die URL und fragt beim entsprechenden VIP-Server nach, ob der Zugriff erlaubt ist.

Wenn für das angeforderte Objekt kein unbeschränkter Zugriff eingestellt ist, muß sich der Benutzer über den Anmeldedialog des Browsers anmelden. (Der unbeschränkte Zugriff auf ein Objekt wird durch die Erlaubnis “Lesen” bzw. “Lesen im Produktionssystem” für “World” (jeder) eingestellt.) Bitte beachten Sie, daß die verschiedenen Browser für den jeweiligen Anmeldedialog unterschiedliche Zeichensätze unterstützen.

Der Webserver sendet die Login-Daten dann an den VIP-Server, der die Login-Daten überprüft und anhand der Zugriffskontrolleinstellungen feststellt, ob der Benutzer die Leseberechtigung für das Objekt besitzt. Ist dies der Fall, wird das Objekt im Browser angezeigt.

Wichtiger Hinweis: Bitte beachten Sie, daß das Zugriffsschutzmodul nur die Webobjekte des VIP-Systems schützt. Alle anderen Dateien unterhalb des VIP-Verzeichnisses (z. B. die des Administrationsservers) müssen deshalb durch andere geeignete Maßnahmen vor unerlaubtem Zugriff gesichert werden.

Anmeldung am VIP-System

Der Zugriffsschutz kann für die verschiedenen VIP-Systeme (Edit, QS, Produktion) unterschiedlich konfiguriert werden. Wenn der Zugriffsschutz für ein System aktiviert ist, muß sich der Benutzer, der eine geschützte Seite im Browser anzeigen möchte, über den Anmeldedialog des Browsers identifizieren. Das gilt auch im Edit- und QS-System. Die Login-Daten werden von den gängigen Browsern (Netscape, Internet Explorer) zwischengespeichert, so daß der Benutzer sich nicht für jede Seite erneut anmelden muß. Wenn der Zugriffsschutz aktiviert ist, ist eine Anmeldung im Edit- und QS-System über den VIP-Anmeldedialog nicht mehr nötig, da VIP die im Browser durchgeführte Anmeldung am Webserver übernimmt. Diese “globale” Anmeldung wird als “Single-Sign-On” bezeichnet.

Dabei ist zu beachten, daß einige Browser (insbesondere Netscape) die Login-Information nicht nur zwischenspeichern, während der Benutzer mit den Seiten des VIP-Systems verbunden ist, sondern so lange, bis die Anwendung komplett beendet wird (*application-wide*). Der Netscape Browser teilt die Login-Daten auch mit den anderen Netscape-Anwendungen (z. B. dem Mailprogramm). Dadurch bleibt die Anmeldung auch nach dem Schließen sämtlicher Browserfenster noch so

lange erhalten, bis alle anderen Netscape-Fenster ebenfalls geschlossen wurden. Wenn Sie sicherstellen möchten, daß die Login-Daten tatsächlich gelöscht sind und damit kein Zugriff auf geschützte Seiten des VIP-Systems ohne erneute Anmeldung mehr möglich ist, müssen sämtliche Netscape-Anwendungen beendet werden.

Das Zwischenspeichern der Login-Informationen wird nicht von jedem Browser bzw. Client-Programm unterstützt. Bei solchen Programmen (z. B. FrontPage 2000) müßte der Benutzer sich für jedes Objekt (also auch für jede Grafik auf einer Seite) neu anmelden. Das Problem kann aber umgangen werden, indem die Single-Sign-On-Funktion abgeschaltet wird. Dadurch wird der Benutzer erst dann aufgefordert, sich anzumelden, wenn er ein Objekt aufruft, bei dem in den Zugriffseinstellungen die Leserechte für “Jeder” fehlen. Das Login erfolgt in diesem Fall nicht über den Anmeldedialog des Browsers bzw. des Client-Programms, sondern über den VIP-Anmeldedialog.

Die Single-Sign-On-Funktion ist standardmäßig eingeschaltet. Um sie abzuschalten, muß in der Properties-Datei

server.properties

der folgende Eintrag hinzugefügt bzw. auf den Wert NO umgestellt werden.

```
...
IMMEDIATE_LOGIN=NO
```

Zugriffsschutz – allgemeine Konfiguration

Bibliotheken und Konfigurationsdateien

Die Bibliotheken und Konfigurationsdateien der Zugriffsschutzkomponente befinden sich nach der Installation in den Unterverzeichnissen von

{VIP-Installationsverzeichnis}\secure

> **Hinweis:** Eine Liste der aktuell unterstützten Bibliotheken des Zugriffsschutzmoduls finden Sie in der Freigabemitteilung.

Konfigurationsdatei pathlist.txt

Die Datei **pathlist.txt** befindet sich nach der Installation im Verzeichnis

{VIP-Installationsverzeichnis}\secure\config

Die Einträge in dieser Datei werden bei der Installation automatisch angepaßt. Je nach gewünschtem Verhalten des Systems sind gegebenenfalls neue Einträge hinzuzufügen (z. B. ein weiteres Mapping für das Produktionssystem) oder die Einträge für einen bestimmten Server zu ändern, insbesondere die Einstellung des Ausfallverhaltens (siehe unten).

```
/edit /edit vip.mustermann.de 20000 VIP-Authorization ⇨
  de.gauss.vip98.server.services.WebAuthorizationService FALSE

/qs /qs vip.mustermann.de 20010 VIP-Authorization ⇨
  de.gauss.vip98.server.services.WebAuthorizationService FALSE

/produktion /produktion vip.mustermann.de 20020 ⇨
  VIP-Authorization ⇨
    de.gauss.vip98.server.services.WebAuthorizationService TRUE

/home /produktion/mustermann/WebSite vip.mustermann.de 20020 ⇨
  VIP-Authorization ⇨
    de.gauss.vip98.server.services.WebAuthorizationService TRUE
```

Diese Einträge sind folgendermaßen aufgebaut:

```
{webserver-mapping} {vip-mapping} {servername} {portnummer} ⇨
  {realm} {vip-service} {verhalten}
```

- `Webserver-Mapping`: Das Verzeichnismapping des Webservers, unter dem der entsprechende VIP-Server zu finden ist. Beispiel: `home`
- `VIP-Mapping`: Das Verzeichnismapping, unter dem die Website-Daten abgelegt sind. Beispiel: `/produktion/mustermann/website`
- `Servername`: Der komplette Name des Servers mit Domain und Erweiterung. Beispiel: `vipserver.mustermann.de`.
- `Portnummer`: Die Portnummer des VIP-Servers. Beispiel: `20000`.
- `Realm`: Dieser Eintrag ist standardmäßig auf `VIP-Authorization` zu setzen.
- `VIP-Service`: Vollständiger Name der VIP-Service-Klasse, die die Überprüfung vornimmt: `de.gauss.vip98.server.services.WebAuthorizationService`.
- `Verhalten`: Das Verhalten bestimmt, ob die angeforderten Objekte grundsätzlich angezeigt werden sollen bzw. wie verfahren wird, wenn der angegebene VIP-Server für die Zugriffskontrolle nicht erreichbar ist und daher keine Überprüfung der Zugriffsrechte durchgeführt werden kann.

  `EXCLUDE` – Dieser Wert gibt an, daß angeforderte Objekte, deren URLs dem Webserver-Mapping entsprechen, grundsätzlich angezeigt werden. Der VIP-Server wird *nicht* zur Überprüfung der Zugriffsrechte herangezogen.

  `TRUE` – Wenn der Webserver den VIP-Server nicht erreichen kann (z. B. beim Ausfall des VIP-Servers), werden die angeforderten Objekte angezeigt.

  `FALSE` – Wenn der Webserver den VIP-Server nicht erreichen kann, werden die angeforderten Objekte nicht angezeigt.

> **Hinweis:** Ist der Wert auf `FALSE` gesetzt, werden überhaupt keine Objekte dieses Servers angezeigt, wenn der Webserver den VIP-Server nicht erreichen kann. Dies gilt auch für die Objekte, bei denen der Zugriff allgemein (ohne Authentifizierung) erlaubt ist.

Das obige Beispiel enthält zwei verschiedene Einträge für den Produktionsserver. Der erste Eintrag bezieht sich auf die ursprüngliche Adresse des Produktionssystems, wie sie bei der Installation festgelegt wurde (z. B. `vip.mustermann.de/produktion`). Der zweite Eintrag ordnet die URL der Homepage (z. B. `vip.mustermann.de/home`) direkt dem obersten Knoten der Website zu (in diesem Fall also: `vip.mustermann.de/produktion/mustermann/WebSite`). Durch diese Art von Mapping (Adressenzuordnung) wird der Zugang zum Produktionssytem erleichtert, da der Benutzer nicht die gesamte URL bis hin zum Website-Knoten im Produktionssystem eingeben muß.

Eine weitere Zuordnungsmöglichkeit wäre:

```
/  /produktion/mustermann/website/ vip.mustermann.de 20020 ⇨
  VIP-Authorization ⇨
    de.gauss.vip98.server.services.WebAuthorizationService TRUE
```

> **Hinweis:** Die gleiche Zuordnung muß auch im Webserver eingestellt sein.

In diesem Fall wird der Wurzelknoten (root directory) der Domäne (z. B. `vip.mustermann.de/`) direkt dem obersten Knoten der Website zugeordnet (`vip.mustermann.de/produktion/mustermann/website/`). Beachten Sie bitte, daß der als VIP-Mapping eingegebene Wert im Falle einer solchen Wurzelzuordnung (root mapping) mit einem Schrägstrich (/) enden muß.

Sie können auch bei der Adressenzuordnung einen vom Webserver explizit belegten Port angeben. Die Zuordnung sieht dann wie folgt aus:

```
/edit :83/edit vip.mustermann.de 20000 VIP-Authorization ⇨
  de.gauss.vip98.server.services.WebAuthorizationService TRUE
```

Hinweis: Wenn bei der VIP-Installation auch Portnummern in den URLs angegeben wurden, enthalten die bei der Installation automatisch erzeugten Einträge in der Datei **pathlist.txt** Zuordnungen von `:{Portnummer}/{Serververzeichnis}` auf `:{Portnummer}/{Serververzeichnis}`.

Beispiel:

```
:83/edit :83/edit vip.mustermann.de 20000 VIP-Authorization ⇨
  de.gauss.vip98.server.services.WebAuthorizationService FALSE
```

Hier muß die Zuordnung angepaßt werden: Die jeweilige Portadresse ist aus dem Webserver-Mapping (dem ersten Wert) zu entfernen.

Fehlerbehandlung

Die Logdatei der DLL bzw. der Shared Library befindet sich (bei einer Standardkonfiguration) in dem Verzeichnis

{VIP-Installationsverzeichnis}\secure

Diese Datei könnte für die Fehlerfindung von Nutzen sein und sollte daher nach dem Auftreten eines Fehlers gesichert werden.

Microsoft-Webserver unter Windows NT 4.0

Vorbereitende Aufgaben

In das Verzeichnis **c:\winnt** muß die Datei **vipauth.ini** kopiert werden. Diese Datei befindet sich nach der Installation im Verzeichnis:

{VIP-Installationsverzeichnis}\secure\config

vipauth.ini

```
[COMMON]
properties={VIP-Installationsverzeichnis}\secure\config\pathlist.txt
logfile={VIP-Installationsverzeichnis}\secure\log.txt
logfileDebug={VIP-Installationsverzeichnis}\secure\logDebug.txt

[NTLM]
user=vipuser
pwd=vipvip
```

Die Einträge unter `[COMMON]` geben an, wo die Property-Datei bzw. das Logfile hinterlegt sind. Die Werte werden bei der Installation automatisch an das System angepaßt. Wenn keine Logdatei geführt werden soll, ist dieser Eintrag nicht nötig.

Mit dem Eintrag `logfileDebug` können Sie die Ausgabe eines Debug-Protokolls aktivieren. Dies ist besonders bei der Neukonfiguration des Zugriffsschutzmoduls bzw. bei der Problemlokalisierung sinnvoll. Im Falle eines korrekt konfigurierten Systems sollten Sie auf das Debug-Protokoll verzichten. Löschen Sie dazu den Eintrag `logfileDebug`.

Der Benutzer, der an dieser Stelle unter `[NTLM]` eingetragen ist, muß neu angelegt und der Gruppe “Gäste” zugeordnet werden. Die Webserver von Microsoft benutzen die Domain-Verwaltung von Windows NT. Ist dieser Benutzer der Domain-Verwaltung von Windows NT nicht bekannt, schlägt auch die Anmeldung am Webserver fehl.

Microsoft Internet Information Server 4.0

Der MIIS 4.0 muß über die Microsoft Management Konsole verwaltet werden. Sollte diese Konsole nicht zur Verfügung stehen, muß das Microsoft Windows NT 4.0 Option Pack installiert werden.

Stellen Sie die Konfiguration des Webservers wie in den folgenden Abbildungen gezeigt ein. Beenden Sie zuvor (über *Systemsteuerung* → *Dienste*) den *WWW-Publishingdienst*. Die Microsoft Management Konsole können Sie dann über das Startmenü aufrufen (Programmgruppe *Internet-Dienst-Manager*).

Hinweis: Bevor Sie die Konfiguration des Webservers verändern, sollten Sie die aktuellen Einstellungen notieren, um gegebenenfalls auf diese zurückgreifen zu können, wenn Probleme beim Konfigurieren auftreten sollten.

Haupteigenschaften-Fenster öffnen

In der *Microsoft Management Konsole* markieren Sie den Computer, auf dem der Webserver konfiguriert werden soll. Wählen Sie aus dem *Kontextmenü* (rechte Maustaste) den Menüpunkt *Eigenschaften*, um den *Eigenschaften*-Dialog aufzurufen.

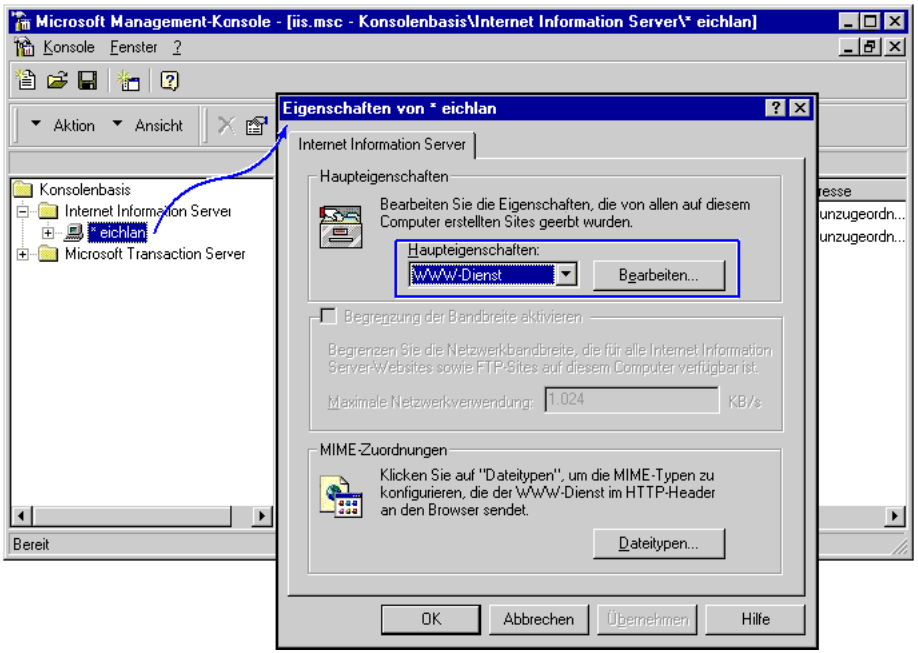

Abb. 12 – Microsoft Management Konsole (MMKS)

Öffnen Sie anschließend das Haupteigenschaften-Fenster. Wählen Sie dazu unter *Haupteigenschaften* den Eintrag *WWW-Dienst*, und klicken Sie auf *Bearbeiten*.

Es erscheint folgender Dialog:

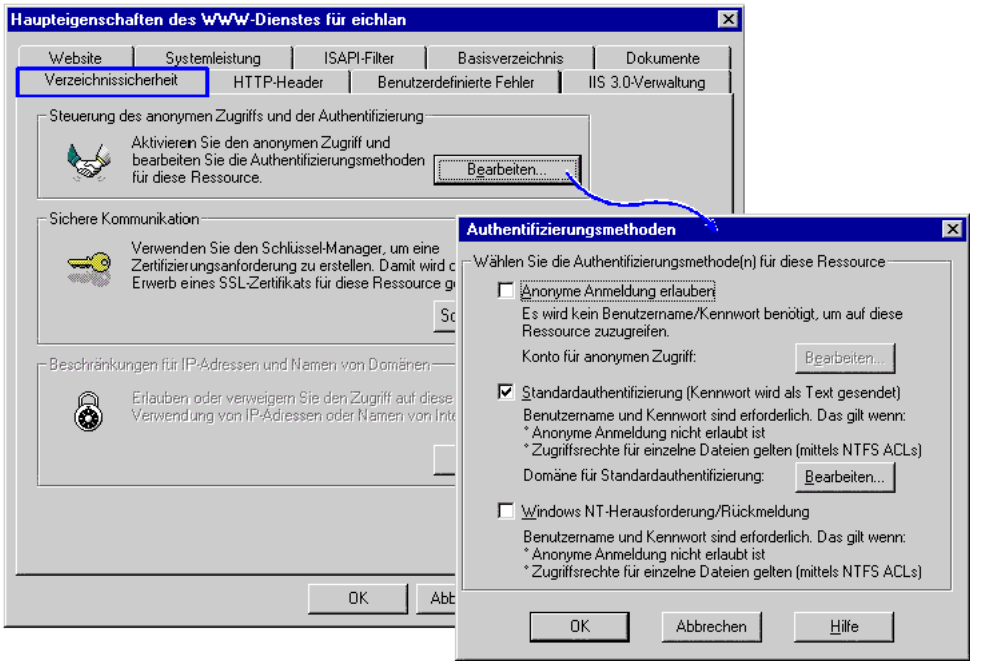
Haupteigenschaften des WWW-Dienstes für eichlan
Website
Systemleistung
ISAPI-Filter
Basisverzeichnis
Dokumente
Verzeichnissicherheit
HTTP-Header
Benutzerdefinierte Fehler
IIS 3.0-Verwaltung
Steuerung des anonymen Zugriffs und der Authentifizierung
Aktivieren Sie den anonymen Zugriff und bearbeiten Sie die Authentifizierungsmethoden für diese Ressource.
Bearbeiten...
Sichere Kommunikation
Verwenden Sie den Schlüssel-Manager, um eine Zertifizierungsanforderung zu erstellen. Damit wird c
Erwerb eines SSL-Zertifikats für diese Ressource g
Beschränkungen für IP-Adressen und Namen von Domänen
Erlauben oder verweigern Sie den Zugriff auf diese
Verwendung von IP-Adressen oder Namen von Int
OK
Abb
Authentifizierungsmethoden
Wählen Sie die Authentifizierungsmethode(n) für diese Ressource
Anonyme Anmeldung erlauben
Es wird kein Benutzername/Kennwort benötigt, um auf diese Ressource zuzugreifen.
Konto für anonymen Zugriff:
Bearbeiten...
Standardauthentifizierung (Kennwort wird als Text gesendet)
Benutzername und Kennwort sind erforderlich. Das gilt wenn:
* Anonyme Anmeldung nicht erlaubt ist
* Zugriffsrechte für einzelne Dateien gelten (mittels NTFS ACLs)
Domäne für Standardauthentifizierung:
Bearbeiten...
Windows NT-Herausforderung/Rückmeldung
Benutzername und Kennwort sind erforderlich. Das gilt wenn:
* Anonyme Anmeldung nicht erlaubt ist
* Zugriffsrechte für einzelne Dateien gelten (mittels NTFS ACLs)
OK
Abbrechen
Hilfe

Abb. 13 – MMKS: Verzeichnissicherheit

Wählen Sie im Haupteigenschaften-Fenster die Seite *Verzeichnissicherheit*, und klicken Sie auf den Button *Bearbeiten*. Im Dialog *Authentifizierungsmethoden* ist die Option *Standardauthentifizierung* zu aktivieren.

> **Hinweis:** Wenn für mehrere Webserver Einstellungen vorgenommen werden sollen, wiederholen Sie diese Schritte für die einzelnen Computer bzw. Server.

ISAPI-Filter einstellen

Wählen Sie im Haupteigenschaften-Fenster die Seite *ISAPI-Filter*, und klicken Sie auf den Button *Hinzufügen* (bzw. *Bearbeiten*).

Im Dialog *Filtereigenschaften* stellen Sie die entsprechenden Parameter ein:

- Geben Sie unter *Filtername* einen Namen ein, mit dem der Filter im VIP-System eindeutig identifiziert werden kann.

- Unter *Programm* muß das Verzeichnis und der Name der DLL angegeben werden.

Hinweis: Angaben zu den Namen der entsprechenden DLLs für die unterstützten Webserver finden Sie in der Freigabemitteilung.

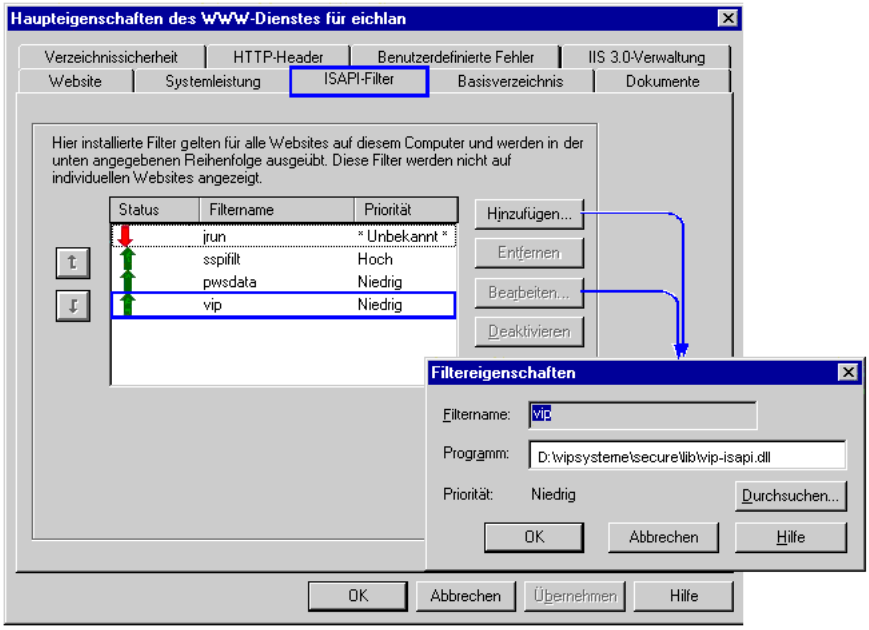

Abb. 14 – MMKS: ISAPI-Filter

Anschließend müssen die beendeten Webserver neu gestartet werden.

Verhalten im Fehlerfall

Während der Laufzeit können zwei unterschiedliche Fehlerzustände auftreten:

- **Ausfall des VIP-Servers:** Das Verhalten beim Ausfall des VIP-Servers wird in der Datei **pathlist.txt** festgelegt, vgl. Abschnitt “Konfigurationsdatei pathlist.txt” auf Seite 64.
- **Absturz der DLL:** Das Verhalten des Webservers beim Absturz der DLL entspricht dem Verhalten, als wäre VIP’Secure nicht installiert, wobei jedoch für jede Anfrage an den Webserver (auch solche, die nicht dem Mapping in der **pathlist.txt** entsprechen) der Login-Dialog des Browsers erscheint. Wird im Login-Dialog ein Benutzer angegeben, der in der NT-Domäne bekannt ist, wird das angeforderte Objekt angezeigt, auch wenn der Benutzer dafür nicht über das Leserecht verfügt.

Um den ursprünglichen Betrieb des Webservers wieder herzustellen, müssen die Webserver-Einstellungen wieder auf ihren alten Stand zurückgesetzt werden.

Netscape Enterprise Server

Die Konfiguration des Netscape Enterprise Servers ist unter Windows NT und Sun Solaris identisch.

Die Datei **obj.conf** im Verzeichnis

{Webserver-Installationsverzeichnis}\SuiteSpot\ https-{Rechnername}\config

muß um folgende Einträge erweitert werden:

```
Init fn="load-modules" shlib="{VIP-Installationsverzeichnis}/secure/lib/ ➪
  {Bibliotheksname}" funcs="VIPAuth_AuthTrans,VIPAuth_PathCheck, ➪
    VIPAuth_Service,VIPAuth_Init"

Init fn="VIPAuth_Init" properties="{VIP-Installationsverzeichnis}/ ➪
  secure/config/pathlist.txt" logFile="{VIP-Installationsverzeichnis}/ ➪
    secure/log.txt"logFileDebug="{VIP-Installationsverzeichnis}/secure/ ➪
      logDebug.txt"

<Object name="default">
...
```

```
AuthTrans fn="VIPAuth_AuthTrans"
AuthTrans fn= ...
...
PathCheck fn="VIPAuth_PathCheck"
PathCheck fn= ...
...
Service fn="VIPAuth_Service"
Service fn= ...
...
</Object>
```

Hinweis: Wenn es für die Objektparameter `AuthTrans`, `PathCheck` und `Service` mehrere Einträge gibt, müssen die hier genannten Einstellungen jeweils an erster Stelle stehen.

Als zusätzlichen Parameter des Eintrags `Init fn="VIPAuth_Init"` können Sie durch das Element `logfileDebug` die Ausgabe eines Debug-Protokolls aktivieren. Dies ist besonders bei der Neukonfiguration des Zugriffsschutzmoduls bzw. bei der Problemlokalisierung sinnvoll. Im Falle eines korrekt konfigurierten Systems sollten Sie auf das Debug-Protokoll verzichten. Löschen Sie dazu den Eintrag `logfileDebug`.

Damit die hier vorgenommenen Änderungen wirksam werden, ist es erforderlich, den HTTP-Server neu zu starten.

Verhalten im Fehlerfall

Während der Laufzeit können zwei unterschiedliche Fehlerzustände auftreten :

- **Ausfall des VIP-Servers:** Das Verhalten beim Ausfall des VIP-Servers wird in der Datei **`pathlist.txt`** festgelegt, vgl. Abschnitt “Konfigurationsdatei `pathlist.txt`” auf Seite 64.
- **Absturz der DLL oder der Shared Library:** Beim Absturz der DLL oder der Shared Library wird der Webserver beendet bzw. kann nicht gestartet werden.

Um den ursprünglichen Betrieb des Webservers wieder herzustellen, müssen die Webserver-Einstellungen auf ihren alten Stand zurückgesetzt werden.

Apache Webserver

Um die VIP-Zugriffsschutzkomponente für den Apache Webserver nutzen zu können, muß die Datei **httpd.conf** im Konfigurationsverzeichnis des Webservers angepaßt werden.

Die folgenden Einträge können am Ende der Konfigurationsdatei vorgenommen werden:

```
LoadModule vipauth_module {VIP-Installationsverzeichnis}\secure\lib\ ➪
  {Bibliotheksname}
AddVIPAuth {VIP-Installationsverzeichnis}\secure\config\pathlist.txt ➪
  {VIP-Installationsverzeichnis}\secure\vipApache.log ➪
    {VIP-Installationsverzeichnis}\secure\vipDebug.log

<Location /{Mapping}>
AuthType Basic
AuthName VIP-Authorization
require valid-user
</Location>

<LocationMatch /(getuser|GETUSER)>
AuthType Basic
AuthName VIP-Authorization
require valid-user
</LocationMatch>
```

Mit dem zweiten Parameter im Eintrag `AddVipAuth` bestimmen Sie, wo die Protokolldatei des Zugriffsschutzmoduls gespeichert werden soll.

Als zusätzlichen Parameter des Eintrags `AddVipAuth` können Sie die Ausgabe eines Debug-Protokolls angeben. Dies ist besonders bei der Neukonfiguration des Zugriffsschutzmoduls bzw. bei der Problemlokalisierung sinnvoll. Im Falle eines korrekt konfigurierten Systems sollten Sie auf das Debug-Protokoll verzichten. Löschen Sie dazu diesen Eintrag.

Hinweis: Unter Solaris und Linux müssen Sie die Zugriffsrechte auf das Verzeichnis, in das die Logdateien geschrieben werden (standardmäßig **{VIP-Installationsverzeichnis}/secure**), so einstellen, daß jeder Benutzer Lese- und Schreibrechte hat (`chmod 666`).

Apache & Solaris

Der Apache-Webserver muß bei der Installation so konfiguriert werden, daß er andere Module einbinden kann. Ist dies nicht der Fall und es wird versucht, den Apache mit dem VIP-Modul zu starten, erscheint folgende Fehlermeldung:

```
Invalid command "LoadModule", perhaps misspelled or defined
by a module not included in the server.
```

Um dieses Problem zu beheben, muß der Apache-Webserver neu übersetzt werden.

> **Wichtiger Hinweis:** Vor dem Übersetzen sollten Sie unbedingt Sicherungskopien Ihrer alten Dateien erstellen.

Das Modul muß bei der Installation mit eingebunden werden. Die Installation des Apache-Webservers würde dann folgendermaßen aufgerufen:

```
./configure –enable-module=so
make
make install
```

4.5 Konfiguration einer LDAP-Anbindung

Durch den Einsatz eines LDAP-Verzeichnisdienstes (Directory Server) kann der Verwaltungsaufwand im Zusammenhang mit der Konfiguration und Pflege von Benutzerdaten erheblich reduziert und die unternehmensweite Konsistenz dieser Daten verbessert werden. Darüber hinaus kann der VIP'ContentManager die Authentifizierung der Benutzer von einem LDAP-Server durchführen lassen. Die Benutzer-, Gruppen- und Rolleninformationen eines existierenden LDAP-Verzeichnisdienstes können vom VIP-Administrationssystem übernommen und genutzt werden. Das VIP-System kann folgende Informationen aus dem Verzeichnisdienst übernehmen:

- Benutzer mit Kennung, Name, Mailadresse, Sprache, Stellvertreter und ggf. Paßwort (siehe unten)
- Gruppen mit Mailadresse und zugeordneten Benutzern
- Rollen mit Mailadresse und zugeordneten Benutzern

Informationen, die im Verzeichnisdienst nicht verfügbar sind oder nicht übernommen werden sollen (z. B. die Paßwörter der Benutzer), können direkt im VIP-Administrationssystem verwaltet werden.

Wichtige Hinweise:

- Paßwörter können in das VIP-System nur übernommen werden, wenn sie im Verzeichnisdienst in Klartext (d. h. unverschlüsselt) abgelegt sind.
- Im VIP-System wird die genaue Schreibweise von Benutzerkennungen und Paßwörtern – unter Berücksichtigung der Groß- und Kleinschreibung – unterschieden.
- Benutzerkennungen, die aus einem LDAP-Verzeichnisdienst ins VIP-System übernommen werden, dürfen nur folgende Zeichen enthalten:

  a-z A-Z 0-9 - (Bindestrich) _ (Unterstrich)

Vorgehensweise im Überblick

Im folgenden wird beschrieben, welche Vorgänge und Einstellungen notwendig sind, um eine Verbindung zum LDAP-Server aufzubauen.

Das Einrichten einer LDAP-Anbindung umfaßt folgende Schritte:

- Sicherung aller Daten der Benutzer-Administration
- Zusätzliche Klassen und Attribute am LDAP-Server einbinden
- LDAP-Server neu starten
- VIP-Server herunterfahren
- Konfigurationsdatei **directory.properties** anpassen
- VIP-Server starten
- Abgleich mit dem LDAP-System durchführen

Schritt 1 – Sicherung aller Daten der Benutzer-Administration

Sichern Sie alle Daten der Benutzer-Administration, die sich im Verzeichnis **...admin\UserAdmin** des VIP-Administrationsservers befinden.

Schritt 2 – Zusätzliche Klassen und Attribute am LDAP-Server einbinden

Für die Übernahme der Benutzerdaten in das VIP-Administrationssystem müssen im Directory-Server zusätzliche Objektklassen und Attribute definiert werden.

Die Objektklassen haben keine speziellen OIDs im Rahmen des X500-Protokolls (LDAP). Es dürfen beliebige OIDs gewählt werden, sofern diese innerhalb des Directory-Servers eindeutig verwendet werden.

Die folgende Tabelle zeigt, welche Attribute zusätzlich im Directory-Server angelegt und welche in der Konfiguration als `required` eingestellt werden müssen. Als Datentyp (Syntax) muß für diese Einträge `Case Ignore String` gewählt werden.

Tabelle 3 – Attribute im Directory-Server

Klasse	Attribut	zusätzlich anlegen	required
Objectclass vip(Parent: top)	vipType[vipUser, vipGroup, vipRole]	✓	✓
	vipAccess[true, false]	✓	✓
Objectclass vipUser(Parent: vip)	uid		✓
	cn		✓
	mail		✓
	preferredLanguage		
	userPassword		
	vipSubstitute	✓	
Objectclass vipGroup(Parent: vip)	cn		✓
	mail		
	member		
Objectclass vipRole(Parent: vip)	cn		✓
	mail		
	member		

Hinweis: Wenn Sie mit einem Active-Directory-Server arbeiten und es nicht möglich ist, Einträge von eigenen Objektklassen anzulegen, können die benötigten Attribute zu bereits bestehenden Objektklassen hinzugefügt werden. Im Syntax-Eingabefeld des Active-Directory-Server ist “Unicode-Zeichenfolge” für ein Attribut zu wählen.

Zur bestehenden Objektklasse `vipUser` werden die Attribute `vipType` und `vipAccess` hinzugefügt. `vipType` entspricht dabei `vipUser`. Diese Attribute werden ebenfalls zur bestehenden Objektklasse `vipGroup` hinzugefügt, wobei `vipType` `vipGroup` bzw. `vipRole` entspricht, je nachdem ob es sich um eine Gruppe oder eine Rolle handelt.

Beim LDAP-Abgleich werden nur die Einträge übernommen, bei denen `vipAccess` auf `TRUE` gesetzt ist.

Schritt 3 – LDAP-Server neu starten

Nach dem Einbinden der zusätzlichen Klassen und Attribute muß der LDAP-Server neu gestartet werden.

Schritt 4 – VIP-Server herunterfahren

Vor dem Anpassen der Einträge in der Konfigurationsdatei **directory.properties** müssen die VIP-Server heruntergefahren werden.

Schritt 5 – Konfigurationsdatei directory.properties anpassen

Die Verbindung zum Verzeichnisdienst (LDAP) wird in der Konfigurationsdatei **directory.properties** konfiguriert. Mit den Einträgen in dieser Datei geben Sie an, ob eine Verbindung zum LDAP-Server aufgebaut werden soll, welche Daten aus dem Verzeichnisdienst gelesen werden sollen, und wo diese Daten im Verzeichnisdienst zu finden sind. Diese Konfigurationsdatei könnte z. B. wie folgt aussehen:

directory.properties

```
# ON  = The directory services of the LDAP server are to be used.
# OFF = The directory services of the LDAP server are not to be used.
# All user administration information will be managed by
# VIP'ContentManager.
LDAP=OFF

# The URL and port of the directory service
URL=ldap://directoryServer.mustermann.de:389

# This value defines the service provider to be used.
# This parameter must be set to the value shown below.
CONTEXT_FACTORY=com.sun.jndi.ldap.LdapCtxFactory
```

```
# This parameter specifies what kind of security check is to be made.
# The possible values are none (no check), simple (simple check) or strong
# (thorough check).
AUTHENTICATION=simple

# This parameter specifies whether direct login is to take place via the
# LDAP server or the VIP server.
# TRUE  = Direct login via LDAP server.
# FALSE = Login to VIP server.
LDAP_LOGIN=TRUE

# The node taken as the starting point for the user search.
LOGIN_BASE=o=mustermann.de
# The user who must be specified so that the search can be run.
LOGIN_USER=Admin
# The password used for authentication.
LOGIN_PWD=admin

# The user profiles from the LDAP server are (not) adopted at every login.
# For this entry it is necessary for the values for GROUP_ROOT and
# ROLE_ROOT to be set.
GET_LDAP_PROFILE=TRUE

# User data is (not) copied.
USER_ACCESSIBLE=TRUE
# Group data is (not) copied.
GROUP_ACCESSIBLE=TRUE
# Role data is (not) copied.
ROLE_ACCESSIBLE=TRUE

# The members of the groups are (not) copied.
GROUP_MEMBERSHIP_ACCESSIBLE=TRUE
# The members of the roles are (not) copied.
ROLE_MEMBERSHIP_ACCESSIBLE=TRUE

# The users substitutes are (not) copied.
SUBSTITUTES_ACCESSIBLE=TRUE

# The users passwords are (not) copied.
# Note: The passwords can only be used if they are filed in plain language
# (i.e. not encrypted).
USER_PASSWORD_ACCESSIBLE=FALSE

# The LDAP descriptor for the user ID (UID).
UID_ATTRIB=uid
# The LDAP descriptor for the user password.
PASSWORD_ATTRIB=userpassword
# The LDAP descriptor for the user e-mail address.
```

```
USER_MAIL_ATTRIB=mail
# The LDAP descriptor for the user name (Common Name).
USER_NAME_ATTRIB=cn
# The LDAP descriptor for the language code.
USER_LANG_ATTRIB=preferredLanguage
# The LDAP descriptor for the substitute.
SUBSTITUTE_ATTRIB=vipSubstitute
# The LDAP descriptor for the group name.
GROUP_NAME_ATTRIB=cn
# The LDAP descriptor for the group e-mail address.
GROUP_MAIL_ATTRIB=mail
# The LDAP descriptor for the role name.
ROLE_NAME_ATTRIB=cn
# The LDAP descriptor for the group e-mail address.
ROLE_MAIL_ATTRIB=mail
# The LDAP descriptor for the group members or role members.
MEMBER_ATTRIB=member

# Enter the search context for the users within a directory service.
USER_ROOT=ou=vipUser, o=mustermann.de
# Enter the search context for the groups within a directory service.
GROUP_ROOT=ou=vipGroup, o=mustermann.de
# Enter the search context for the roles within a directory service.
ROLE_ROOT=ou=vipRole, o=mustermann.de

# These parameters allow you to specify the scope of the search context:
# SUBTREE_SCOPE searches the entire tree below the specified node (e.g.
# USER_ROOT), whereas ONELEVEL_SCOPE searches only the level directly
# below
# the node.
SEARCH_SCOPE=SUBTREE_SCOPE

# This parameter describes the structure of the DN (Distinguished Name).
# The asterisk (*) is replaced by the user specified under LDAP Login name
# in the LDAP panel of the VIP Administration system. The DN determined in
# this way is used to login to the LDAP server during the update process.
LDAP_ADMIN_NAME_TEMPLATE=cn=*

# When deleting users, roles or groups a check is (not) made to see whether
# they are still entered in an ACL (Access Control List). If they are
# present in the ACL, they cannot be deleted.
LDAP_UPDATE_QUERY_EDIT_SERVER=TRUE
```

Allgemeine Einstellungen

LDAP=ON | OFF

ON — Die Verzeichnisdienste des LDAP-Servers sollen verwendet werden

OFF — Die Verzeichnisdienste des LDAP-Servers sollen nicht verwendet werden. Alle Informationen der Benutzer-Administration werden durch den VIP'ContentManager verwaltet.

URL=server.domain.ext:port

Die URL und der Port des Verzeichnisdienst-Servers, zum Beispiel: `URL=directoryServer.mustermann.de:389`

CONTEXT_FACTORY=com.sun.jndi.ldap.LdapCtxFactory

Mit diesem Wert wird der zu verwendende Service Provider festgelegt. Dieser Parameter muß auf den o. a. Wert eingestellt sein.

AUTHENTICATION=none | simple | strong

Mit diesem Parameter wird festgelegt, welche Art der Sicherheitsprüfung durchgeführt wird. Als Wert kann `none` (keine Prüfung), `simple` (einfache Prüfung) oder `strong` (intensive Prüfung) angegeben werden.

LDAP_LOGIN=TRUE | FALSE

Mit diesem Parameter wird festgelegt, ob ein direktes Einloggen über den LDAP-Server oder über den VIP-Server erfolgt.

TRUE — Das direkte Einloggen wird über den LDAP-Server durchgeführt. In diesem Fall müssen die Werte `UID_ATTRIB` und `USER_ROOT` ebenfalls gesetzt sein.

FALSE — Das Einloggen erfolgt am VIP-Server.

LOGIN_BASE=o=mustermann.de

Der Startknoten, unter dem der Benutzer zunächst gesucht wird. Wenn ein Startknoten angegeben wird, müssen die Werte für `LOGIN_USER` und `LOGIN_PWD` ebenfalls gesetzt sein.

`LOGIN_USER=Admin`

Der Benutzer, der angegeben werden muß, damit die Suche durchgeführt werden kann.

`LOGIN_PWD=admin`

Das Paßwort, mit dem die Authentifizierung – nach Ermittlung des DN – durchgeführt wird.

`GET_LDAP_PROFILE=TRUE | FALSE`

Die Benutzerprofile vom LDAP-Server werden (nicht) bei jedem Einloggen übernommen. Für diesen Eintrag ist es notwendig, daß die Werte für `GROUP_ROOT` und `ROLE_ROOT` sowie für `LOGIN_USER` und `LOGIN_PWD` gesetzt sind.

Hinweis: Es gelten folgende Einschränkungen, wenn das Benutzerprofil vom LDAP-Server gelesen wird:

- Das Einloggen als Administrator ist nicht möglich.
- Das Einloggen als Stellvertreter ist nicht möglich.
- Die Mitglieder einer Gruppe oder Rolle müssen mit dem DN (Distinguished Name) abgelegt werden. Darüber hinaus muß der Attributbezeichner `member` oder `uniquemember` sein.
- Die Benutzer müssen einer Website *direkt* zugeordnet werden, da das indirekte Zuordnen über Gruppen und Rollen zu einer Website nicht durchgeführt werden kann.

Vorgaben für vom LDAP-Server zu übernehmende Daten

Die folgenden Einstellungen legen fest, welche Daten vom LDAP-Server übernommen werden. Wird ein Parameter auf `TRUE` gesetzt, werden die Daten aus LDAP gelesen. Wird er auf `FALSE` gesetzt, werden die Daten nicht vom LDAP-Server übernommen und müssen vom VIP'ContentManager verwaltet werden.

`USER_ACCESSIBLE=TRUE | FALSE`

Benutzerdaten werden (nicht) übernommen.

`GROUP_ACCESSIBLE=TRUE | FALSE`

Gruppendaten werden (nicht) übernommen.

`ROLE_ACCESSIBLE=TRUE | FALSE`

Rollendaten werden (nicht) übernommen.

`GROUP_MEMBERSHIP_ACCESSIBLE=TRUE | FALSE`

Die Mitglieder der Gruppen werden (nicht) übernommen.

`ROLE_MEMBERSHIP_ACCESSIBLE=TRUE | FALSE`

Die Mitglieder der Rollen werden (nicht) übernommen.

`SUBSTITUTES_ACCESSIBLE=TRUE | FALSE`

Die Stellvertreter der Benutzer werden (nicht) übernommen.

`USER_PASSWORD_ACCESSIBLE=TRUE | FALSE`

Die Paßwörter der Benutzer werden (nicht) übernommen.

> **Hinweis:** Die Übernahme der Paßwörter ist nur möglich, wenn diese in Klarschrift (d. h. unverschlüsselt) abgelegt sind.

`UID_ATTRIB=uid`

Der LDAP-Bezeichner für die Benutzerkennung (UID).

`PASSWORD_ATTRIB=userpassword`

Der LDAP-Bezeichner für das Benutzerpaßwort.

`USER_MAIL_ATTRIB=mail`

Der LDAP-Bezeichner für die Benutzer-Email-Adresse.

`USER_NAME_ATTRIB=cn`

Der LDAP-Bezeichner für den Benutzernamen (Common Name).

`USER_LANG_ATTRIB=preferredLanguage`

Der LDAP-Bezeichner für die Sprachkennung.

`SUBSTITUTE_ATTRIB=vipSubstitute`

Der LDAP-Bezeichner für den Stellvertreter.

`GROUP_NAME_ATTRIB=cn`

Der LDAP-Bezeichner für den Gruppennamen.

`GROUP_MAIL_ATTRIB=mail`

Der LDAP-Bezeichner für die Gruppen-Email-Adresse.

`ROLE_NAME_ATTRIB=cn`

Der LDAP-Bezeichner für den Rollennamen.

`ROLE_MAIL_ATTRIB=mail`

Der LDAP-Bezeichner für die Rollen-Email-Adresse.

`MEMBER_ATTRIB=member`

Der LDAP-Bezeichner für die Gruppen- bzw. Rollenmitglieder.

Vorgaben für die Struktur des Verzeichnisdienstes (Suchkontext)

Durch die folgenden Einträge geben Sie an, wo die entsprechenden Informationen (für Benutzer, Gruppen und Rollen) in der Verzeichnisdienststruktur abgelegt sind. Der Suchkontext für die Benutzer, Gruppen und Rollen muß nicht identisch sein.

`USER_ROOT=ou=bereich,o=firma.de`

Geben Sie hier den Suchkontext für die Benutzer innerhalb des Verzeichnisdienstes an.

`GROUP_ROOT=ou=bereich,o=firma.de`

Geben Sie hier den Suchkontext für die Gruppen innerhalb des Verzeichnisdienstes an.

ROLE_ROOT=ou=bereich,o=firma.de

Geben Sie hier den Suchkontext für die Rollen innerhalb des Verzeichnisdienstes an.

SEARCH_SCOPE=SUBTREE_SCOPE | ONELEVEL_SCOPE

Mit diesem Parameter bestimmen Sie die Reichweite des Suchkontextes: SUBTREE_SCOPE durchsucht den kompletten Baum unterhalb des angegebenen Knotens (z. B. USER_ROOT), während ONELEVEL_SCOPE nur die Ebene direkt unterhalb des Knotens durchsucht.

LDAP_ADMIN_NAME_TEMPLATE=cn=*

Mit diesem Parameter wird der Aufbau des DN (Distinguished Name) beschrieben. Der Stern (*) wird durch den unter *LDAP-Loginname* angegebenen Benutzer im *LDAP*-Panel des VIP-Administrationssystems ersetzt. Mit dem ermittelten DN wird das Einloggen am LDAP-Server beim Abgleich durchgeführt.

LDAP_UPDATE_QUERY_EDIT_SERVER=TRUE | FALSE

Beim Löschen von Benutzern, Rollen oder Gruppen wird (nicht) überprüft, ob diese noch in einer ACL (Access Control List) eingetragen sind. Wenn sie in der ACL vorhanden sind, können sie nicht gelöscht werden.

Schritt 6 – VIP-Server starten

Da die Konfigurationsdateien nur beim Start der VIP-Server gelesen werden, müssen die Server nach dem Anpassen der Einträge in der Datei **directory.properties** neu gestartet werden.

Schritt 7 – Datenabgleich mit dem LDAP-Server durchführen

Nachdem eine Verbindung zum LDAP-Server hergestellt wurde, können Daten aus dem Verzeichnisdienst übernommen werden. Informationen zum Durchführen des Datenabgleichs finden Sie im Abschnitt 5.7 “Datenabgleich mit dem LDAP-Server” auf Seite 160. Die entsprechende Kommandozeile zum Durchführen des Datenabgleichs finden Sie im folgenden Abschnitt.

Hinweis: Beim Abgleich mit einem Active-Directory-Server kann eine PartialException auftreten, wenn *keine* ou (organizational unit) in den Parametern USER_ROOT, GROUP_ROOT bzw. ROLE_ROOT in der Datei **directory.properties** angegeben ist.

LDAP Batch-Abgleich

Durch den Batch-Abgleich mit einem LDAP-System können die Benutzerdaten des VIP-Systems mit den im Verzeichnisdienst (LDAP) enthaltenen Daten abgeglichen werden.

Die Skripte liegen im admin-Verzeichnis und haben die Namen **ldap_update.bat** und **ldap_update.sh**.

Aufruf

```
ldap_update.bat {vip_login} {vip_password} {ldap_login} {ldap_password}
```

Die Aufrufparameter sind in der vorgegebenen Reihenfolge einzugeben. Sie haben folgende Bedeutung:

{vip_login}	Kennung des Adminbenutzers im VIP-System
{vip_password}	Paßwort des Adminbenutzers im VIP-System
{ldap_login}	Kennung des Adminbenutzers im LDAP-Server
{ldap_password}	Paßwort des Adminbenutzers im LDAP-Server

Hinweise:

Im Zusammenhang mit dem LDAP-Batch-Abgleich ist auf folgende Punkte zu achten:

- Wenn ldap_update nicht interaktiv aufgerufen wird, muß stdout und stderr durch Angabe entsprechender Ausgabedateien umgeleitet werden:

```
ldap_update admin AdMiN ladmin LaDmIn > update.out 2> update.err
```

- Nach dem Installieren gilt der JDK-Pfad (PATH) nur für den Installationsrechner!
- Die Batch-Dateien können nur an einer anderen Stelle oder auf einem anderen System ausgeführt werden, wenn dort auch die folgenden JAR-Dateien verfügbar sind (ggf. müssen Sie die JAR-Dateien dorthin kopieren):

  ./java/vipadmin.jar

  ./lib/jndi.jar

  ./lib/ldap.jar

  ./lib/providerutil.jar
- Beachten Sie auch, daß die in den Batch- bzw. Shell-Dateien enthaltenen Pfade ggf. angepaßt werden müssen, wenn Sie die Dateien an eine andere Stelle oder auf ein anderes System kopieren.

4.6 Datenbankanbindung

In diesem Abschnitt wird die Datenbankanbindung (DBC) des VIP-Systems beschrieben. Standardmäßig werden Verwaltungsdaten und Objektinformationen einer Website im Dateisystem (genauer gesagt in CSV-Tabellen) gespeichert. Durch Änderungen in der Konfiguration des VIP-Systems bzw. der Website kann die Datenhaltung auf datenbankgestützte Speicherung eingestellt werden. Besonders bei sehr großen Websites – z. B. Websites mit mehr als 10 000 Objekten – kann es vorteilhaft sein, mit der datenbankgestützten Datenhaltung zu arbeiten.

Durch eine Verdrängungsstrategie für die Speicherbelegung können in einer an eine Datenbank angebundenen Website beliebig viele Objekte verwaltet werden, ohne daß die Objektinformationen sämtlicher Objekte (als CSV-Dateien) ständig im Speicher gehalten werden müssen. Dadurch wird besonders bei sehr großen Websites die Performance verbessert.

Eine Datenbankanbindung wird in erster Linie durch Änderungen in den Konfigurationsdateien des VIP-Systems eingerichtet. Gegebenenfalls muß aber auch die

Konfiguration der Datenbank angepaßt werden. Die erforderlichen Einstellungen zur Konfiguration des VIP-Systems und der verschiedenen Datenbanksysteme werden in den folgenden Abschnitten beschrieben.

Wichtige Hinweise:

- Wenn eine Datenbankanbindung der VIP-Server verwendet wird, sind folgende Konventionen hinsichtlich des Website-Namens zu beachten:
  - Der Name einer Website darf nur folgende Zeichen enthalten: a-z, A-Z, 0-9, **keine** Umlaute bzw. “ß”
  - Am **Anfang** eines Website-Namens dürfen die Ziffern 0-9 **nicht** verwendet werden!
  - Bitte beachten Sie, daß beim Anlegen einer Website die in früheren Versionen erlaubten Zeichen -(Bindestrich), _(Unterstrich) und .(Punkt) im Website-Namen ab der Version 5e.03 **nicht** mehr erlaubt sind. Bei Websites, die in einer früheren Version angelegt wurden und deren Namen die aufgeführten Zeichen enthalten, ist eine einwandfreie Funktionsweise jedoch gewährleistet.
- Aufgrund der sehr unterschiedlichen Eigenschaften der dateibasierten und der datenbankbasierten Datenspeicherung können bestehende Websites nicht ohne weiteres auf Datenbankspeicherung umgestellt werden. Eine solche Umstellung darf nur mit Unterstützung der Gauss Interprise AG vorgenommen werden.
- Die Einrichtung einer Datenbankanbindung der VIP-Server erfordert fundierte Kenntnisse in der Administration des VIP-Systems und des eingesetzten Datenbanksystems.

Grundlagen

Objektinformationen

Zu jedem in einem VIP-System verwalteten Objekt gibt es – neben dem Inhalt, dem Logfile und der aus dem Objekt generierten HTML-Datei – eine Reihe von Attributen, die zur Verwaltung und Klassifizierung der Objekte dienen. Diese Objektattribute werden Metadaten genannt. Ein Teil der Metadaten ist für alle Objekttypen gleich. Es gibt jedoch auch spezielle Metadaten (die sogenannten dynamischen Attribute), die für jeden Objekttyp unterschiedlich definiert sein können. Auch die Informationen zur Steuerung des Zugriffs (ACLs) zählen zu den Attributen eines Objekts.

Bei der dateibasierten Datenhaltung werden diese Objektinformationen in CSV-Tabellen gespeichert, die in den Tables-Verzeichnissen der jeweiligen Websites abgelegt sind, z. B. auf dem Edit-Server unter

{VIP-Installationsverzeichnis}\edit\{Websitename}\Tables

Bei einer Datenbankanbindung werden diese Verwaltungsdaten und Objektattribute in der Datenbank gespeichert.

Architektur des VIP’DBC-Systems

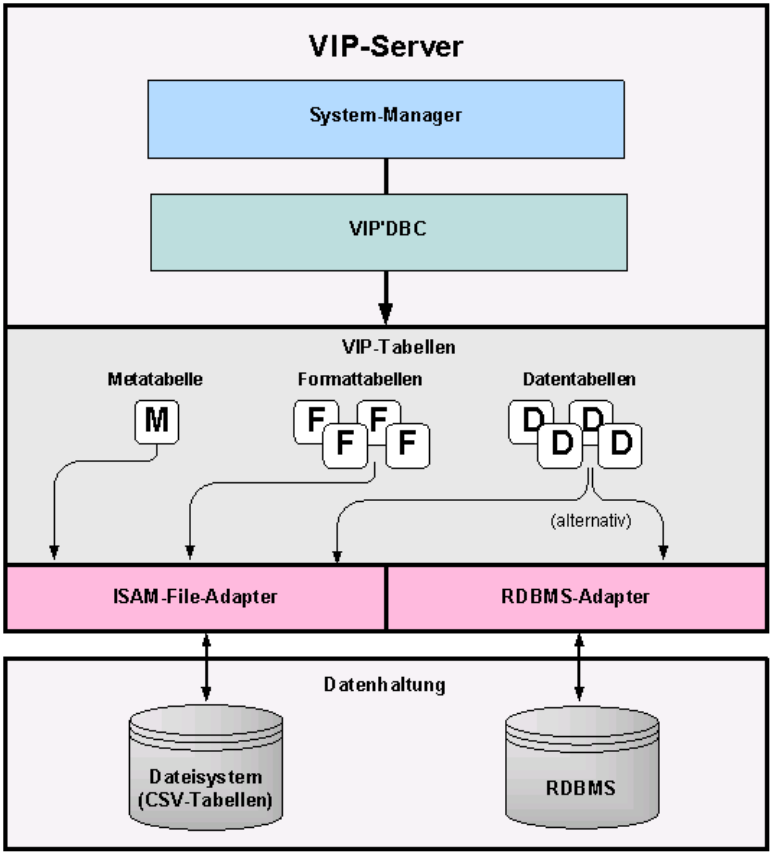

Abb. 15 – VIP’DBC Systemüberblick

Die Metadaten einer Website sind in drei verschiedenen Kategorien von Tabellen gespeichert, nämlich einer Metatabelle (M), den eigentlichen Datentabellen (D) und den jeweiligen Formattabellen (F).

- **Metatabelle:** In dieser Tabelle (**meta.csv**) speichert das VIP’DBC-System seine Konfigurationen ab. Die Metatabelle ist eine CSV-Tabelle mit Zugriffsschlüsseln; sie beinhaltet also zu jeder eingetragenen Tabelle einen Key sowie Metainformationen.

- **Formattabellen:** In den Formattabellen (***_fmt.csv**) wird der Aufbau der einzelnen Tabellen festgelegt.
- **Datentabellen:** In den Datentabellen (***.csv**, außer den oben aufgeführten) sind die Attribute und Verwaltungsinformationen aller Objekte der Website gespeichert.

Der Zugriff auf die Datentabellen erfolgt über einen Treiber. Der zu verwendende Treibertyp ist in der Metatabelle eingetragen. Zur Zeit existieren drei Treibertypen:

- **CSV-Treiber**

  Dieser Treiber verwaltet Dateien, in denen die Daten durch Trennzeichen (;) separiert sind. Die Daten der Tabelle können mit diesem Treibertyp nicht manuell bearbeitet werden (Datensätze hinzufügen, ändern oder löschen).

- **ISAM-Treiber**

  Der ISAM-Treiber verwaltet ebenfalls Dateien, deren Daten durch Trennzeichen (;) separiert sind. Es muß ein Schlüsselfeld definiert werden, das als Primär-Index verwaltet wird. Dieser Treibertyp wird für die Formattabellen des Systems und für die VIP-spezifischen Tabellen verwendet. In diesen Tabellen können Daten manuell bearbeitet werden.

  Hinweis: Bei UNIX-Systemen muß das `ulimit` entsprechend angepaßt werden (`ulimit -n 1024`), da sehr viele Dateien offengehalten werden.

- **JDBC-Treiber**

  Der JDBC-Treiber kann auf jede JDBC- oder ODBC-fähige Datenbank zugreifen. Es müssen bestimmte Metainformationen zu diesem Treiber eingetragen werden, um auf die Datenquelle zugreifen zu können. Danach stehen die gleichen Methoden auf Datensatzebene zur Verfügung wie beim ISAM-Treiber.

Konfiguration einer Datenbankanbindung

Im folgenden Abschnitt werden die notwendigen Einstellungen beschrieben, um die Metainformationen einer Website in einer Datenbank abzulegen.

Hinweise:

Im Zusammenhang mit der Konfiguration einer Datenbankanbindung müssen folgende Hinweise unbedingt berücksichtigt werden:

- Nach dem Einrichten einer Datenbankanbindung gibt es keine Möglichkeit, die Website-Konfiguration auf dateibasierte Datenhaltung zurückzustellen.
- Die Konfiguration einer Datenbankanbindung darf nur von qualifizierten Personen mit entsprechenden Systemkenntnissen (insbesondere in bezug auf das Datenbanksystem und das VIP-System) durchgeführt werden.
- Der temporäre Speicherbereich des Datenbanksystems muß groß genug sein, um eine sichere Abwicklung der Datenspeicherung zu gewährleisten.
- Vor jeder Konfigurationsänderung ist eine **komplette Datensicherung** des VIP-Systems durchzuführen.
- In der Konfigurationsdatei **dbdefinition.properties** werden der Aufbau von Datenbanktabellen in verschiedenen Datenbanksystemen sowie die Kommunikation mit diesen Systemen spezifiziert. In dieser Datei dürfen Sie keine Änderungen vornehmen, da eine einwandfreie Funktionsweise des VIP-Systems dann nicht mehr gewährleistet ist.
- Eine Änderung der Datenquelle ist nach dem Anlegen der Website nicht mehr möglich.
- Beim Löschen einer Website werden die erzeugten Tabellen automatisch aus der Datenbank entfernt.

Vorgehensweise im Überblick

Das Einrichten einer Website mit Datenbankanbindung umfaßt folgende Schritte:

- Datenbank anlegen
- Edit- und QS-Server herunterfahren
- Datensicherung der VIP-Systeme
- Konfigurationsdatei **websites.properties** anpassen
- Formattabellen anpassen
- Alle VIP-Server starten
- Website anlegen

Die einzelnen Schritte werden im folgenden näher beschrieben.

Schritt 1: Datenbank anlegen

Bevor Sie eine Datenbankanbindung konfigurieren können, müssen Sie als erstes die zu verwendende Datenbank anlegen. In den folgenden Schritten wird davon ausgegangen, daß ein funktionierendes, korrekt konfiguriertes Datenbanksystem zur Verfügung steht. Weitere Informationen zur Konfiguration von Datenbanken finden Sie unter “Einrichten von JDBC- bzw. JDBC-ODBC-Datenquellen” auf Seite 102.

Es werden u. a. folgende Datenbanksysteme unterstützt:

- Oracle
- DB2
- Microsoft SQL Server
- Sybase

Hinweis: Angaben zu den Versionen der unterstützten Datenbanksysteme sowie den erforderlichen JDBC- bzw. ODBC-Treibern sind in der Freigabemitteilung enthalten.

Schritt 2: Edit- und QS-Server herunterfahren

Die Server müssen heruntergefahren werden, um sicherzustellen, daß die VIP-Systeme in einem konsistenten Zustand gesichert werden (siehe Schritt 3). Beachten Sie bitte, daß die Serverkonfigurationen nur beim Hochfahren der Server gelesen werden.

Schritt 3: Datensicherung der VIP-Systeme

Bevor Sie mit der Umstellung auf ein datenbankbasiertes System beginnen, ist unbedingt ein Backup des kompletten VIP-Systems zu erstellen. Dazu kopieren Sie das gesamte VIP-Installationsverzeichnis mit allen Unterverzeichnissen auf ein Datensicherungsmedium (z. B. ein Sicherungsband).

Schritt 4: Konfigurationsdatei `websites.properties` anpassen

Diese Datei enthält Einträge zur Konfiguration der VIP-Server und den dazugehörigen Websites. (Die tatsächliche Reihenfolge der Einträge kann von der im folgenden Beispiel angegebenen Reihenfolge abweichen.)

```
ADMIN_HOST =          vipserver.mustermann.de
ADMIN_ADRESSE =       http://vipserver.mustermann.de/admin
ADMIN_PORT =          22030
ADMIN_HTTP =          22031

EDIT_HOST =           vipserver.mustermann.de
EDIT_ADRESSE =        http://vipserver.mustermann.de/edit
EDIT_PORT =           22000
EDIT_HTTP =           22001

QS_HOST =             vipserver.mustermann.de
QS_ADRESSE =          http://vipserver.mustermann.de/qs
QS_PORT =             22010
QS_HTTP =             22011

PRODUKTION_HOST =     vipserver.mustermann.de
PRODUKTION_ADRESSE = http://vipserver.mustermann.de/produktion
PRODUKTION_PORT =     22020
PRODUKTION_HTTP =     22021

OM =             de.gauss.vip98.server.objectmanager.VipObjectManager
SM =             de.gauss.vip98.server.systemmanager.VipFileSystemManager

[www]
WEBSITENAME =    www
```

Die Datei ist in mehrere Abschnitte gegliedert: einen allgemeinen Abschnitt (oben) und spezifische Abschnitte für jede Website (unten). Die Konfiguration einer Website setzt sich aus Website-spezifischen und allgemeinen Einstellungen zusammen, wobei die Website-spezifischen eine höhere Priorität haben.

Durch die Einträge `OM` und `SM` werden für jede Website ein Object-Manager (OM) und ein System-Manager (SM) eingestellt. Da in diesem Beispiel die Einträge `OM` und `SM` nicht im Website-Abschnitt enthalten sind, gelten die allgemeinen Einträge, die eine dateibasierte Speicherung der Systemdaten auf Basis des *VipFileSystemManager* vorsehen. Der VipFileSystemManager ist besonders auf die Speicherung im Dateisystem abgestimmt, da er (zur Reduzierung der Dateisystemzugriffe) ohne Verdrängung von Daten aus dem Hauptspeicher operiert.

Um für eine neue Website eine Verbindung zu einer Datenbank einzurichten, müssen einmalig mehrere allgemeine Einträge (die DBC-Einträge) vorgenommen werden, mit denen die Datenquelle für die Datenbankanbindung spezifiziert wird. (Diese Einträge müssen nur einmal vorgenommen werden und können in der Datei verbleiben oder wieder entfernt werden, nachdem eine neue Website eingerichtet wurde.)

```
DBCDATASOURCE = jdbc:oracle:thin:@vip_server:1521:vip
DBCUSER =       vip
DBCPASSWORD =   contentmanager
DBCPARAMETER =  oracle.jdbc.driver.OracleDriver
DBCMIGRATION =  YES
DBCDBMSTYPE =   ORACLE
```

Um die Vorteile einer datenbankgestützten Speicherung zu nutzen (insbesondere die Performance-Vorteile durch Nutzung der Verdrängungsstrategie), muß im allgemeinen Abschnitt ein anderer System-Manager eingetragen werden:

```
OM =            de.gauss.vip98.server.objectmanager.VipObjectManager
SM =            de.gauss.vip98.server.systemmanager.VipDBSystemManager
FIRST_CACHE =   10000
CHUNK_SIZE =    2000
```

Der VipDBSystemManager unterstützt die Verdrängungsstrategie, d. h. es werden nur die Systemdaten der zuletzt aufgerufenen Objekte im Hauptspeicher gehalten.

Dazu werden Angaben für die Größen des Caches und der Chunk-Size benötigt. (Siehe “Einstellung der Speicherstrategie (Verdrängung)” auf Seite 107.)

Damit die Website www die ursprünglichen Object- und System-Manager behält, müssen die entsprechenden Einträge in den website-spezifischen Abschnitt der Properties-Datei kopiert werden. Die Datei würde dann z. B. so aussehen:

```
ADMIN_HOST =          vipserver.mustermann.de
ADMIN_ADRESSE =       http://vipserver.mustermann.de/admin
ADMIN_PORT =          22030
ADMIN_HTTP =          22031

EDIT_HOST =           vipserver.mustermann.de
EDIT_ADRESSE =        http://vipserver.mustermann.de/edit
EDIT_PORT =           22000
EDIT_HTTP =           22001

QS_HOST =             vipserver.mustermann.de
QS_ADRESSE =          http://vipserver.mustermann.de/qs
QS_PORT =             22010
QS_HTTP =             22011

PRODUKTION_HOST =     vipserver.mustermann.de
PRODUKTION_ADRESSE =  http://vipserver.mustermann.de/produktion
PRODUKTION_PORT =     22020
PRODUKTION_HTTP =     22021

OM =             de.gauss.vip98.server.objectmanager.VipObjectManager
SM =             de.gauss.vip98.server.systemmanager.VipDBSystemManager
FIRST_CACHE =    10000
CHUNK_SIZE =     2000

DBCDATASOURCE =  jdbc:oracle:thin:@vip_server:1521:vip
DBCUSER =        vip
DBCPASSWORD =    contentmanager
DBCPARAMETER =   oracle.jdbc.driver.OracleDriver
DBCDBMSTYPE =    ORACLE
DBCMIGRATION =   YES

[www]
WEBSITENAME =   www
OM =            de.gauss.vip98.server.objectmanager.VipObjectManager
SM =            de.gauss.vip98.server.systemmanager.VipFileSystemManager
```

DBC-Parameter

Die DBC-Parameter haben folgende Bedeutung:

- DBCDATASOURCE spezifiziert die Datenquelle. Im Falle von ODBC-Datenquellen ist diese immer JDBC:ODBC:{dataSourceName}. Dabei steht {dataSourceName} für den in der ODBC-Konfiguration vergebenen Namen.
- DBCUSER und DBCPASSWORD spezifizieren die Benutzerkennung und das Kennwort, das von VIP für die Anmeldung an der Datenbank verwendet wird. Es empfiehlt sich, in der Datenbank dafür eine eigene Kennung anzulegen. Die Kennung und das entsprechende Paßwort müssen in Klartext in der Datei **websites.properties** angegeben werden. Wenn die Datenquelle (z. B. Microsoft SQL Server) keine Benutzeranmeldung benötigt, bleiben die Einträge leer.
- DBCPARAMETER spezifiziert für das DBMS den Klassennamen eines nativen JDBC-Treibers, der vom Hersteller zu beziehen ist. Alternativ kann DBCPARAMETER leer bleiben, wenn das DBMS über die Standard-JDBC-ODBC-Bridge angebunden wird.
- DBCMIGRATION muß auf den Wert YES gesetzt werden, damit die Migration auf datenbankbasierte Datenhaltung nach dem Anlegen der Website durchgeführt wird.

  > **Hinweis:** Es wird empfohlen, die Logging-Dateien und den Parameter DBCMIGRATION nach der Migration zu überprüfen. Nur nach einer erfolgreichen Migration wird er auf DONE gesetzt. Im Fehlerfall wird DBCMIGRATION auf FAILED gesetzt.

- DBCDBMSTYPE spezifiziert das Datenbanksystem, das verwendet werden soll. Verwenden Sie für diesen Eintrag einen der folgenden Werte: MSSQL, ORACLE, DB2, SYBASE. Bitte beachten Sie unbedingt die Schreibweise in Großbuchstaben.

  Informationen zur JDBC- bzw. JDBC-ODBC-Konfiguration finden Sie im Abschnitt “Einrichten von JDBC- bzw. JDBC-ODBC-Datenquellen” auf Seite 102.

Schritt 5: Formattabellen anpassen

Für jede Tabelle existiert eine Formattabelle, in der die Attribute der Tabelle beschrieben sind. Die Formattabellen sind immer als CSV-Dateien abgelegt. Sie werden auch zum Aufbau der Datenhaltung in Datenbanken benötigt.

Möglicherweise müssen bestimmte Formattabellen angepaßt werden, damit die individuellen Grenzen der verschiedenen DBMS (z. B. bei der maximalen Länge von VARCHAR-Feldern oder der maximalen Länge von indizierten Feldern) nicht überschritten werden. Während der Migration einer Website in ein DBMS prüft das VIP-System, ob die Grenzen des DBMS eingehalten werden. Das Ergebnis wird in den Logging-Dateien des jeweiligen VIP-Systems angegeben. Die Prüfung berücksichtigt die bekannten Grenzwerte der unterstützten DBMS. Falls die Migration aufgrund einer Überschreitung der systemspezifischen Grenzen nicht durchgeführt wird, ist der Grund dafür in den Logging-Dateien angegeben.

Da die Eigenschaften und Grenzwerte von DBMS herstellerspezifisch sind und sich auch innerhalb der einzelnen Versionen eines Herstellers stark unterscheiden, kann eine erfolgreiche Migration erst dann zugesichert werden, wenn eine neue Website fehlerfrei angelegt werden konnte. Daher sollte zunächst eine Beispiel- bzw. Test-Website eingerichtet werden, bevor die eigentliche Website eingerichtet wird. Die Test-Website kann nach erfolgreichem Test über das Administrationssystem wieder entfernt werden.

Wichtige Hinweise:

- Die zu ändernden CSV-Dateien müssen vor dem Anpassen gesichert werden.
- Die hier beschriebenen Änderungen an den Formattabellen müssen *in der Master-Website* vorgenommen werden.
- Der Name einer Formattabelle wird aus dem Namen der jeweiligen Datentabelle abgeleitet, indem an den Basisnamen die Zeichenfolge **_fmt** angehängt wird. Beispielsweise heißt die Formattabelle der Objekttabelle **objekte_fmt.csv**.
- In den Formattabellen sind u. a. die benötigten Datentypen, die Größe der Datenfelder und die Information hinterlegt, ob ein Attribut indiziert ist oder nicht. Normalerweise müssen die Formattabellen nicht angepaßt werden. Es ist jedoch möglich, daß die definierten Formate nicht kompatibel zur

verwendeten Datenbank sind. Insbesondere kann es sein, daß der Datentyp eines Attributs bzw. seine Länge angepaßt werden muß.

- Änderungen an den Formattabellen müssen immer mit großer Vorsicht und mit Sachverstand erfolgen.

Im folgenden sind einige Fälle aufgeführt, bei denen Änderungen durchgeführt werden müssen:

- Beim Microsoft SQL Server 6.5 können Character-Felder nicht mehr als 255 Zeichen umfassen. Dadurch entstehen Probleme mit drei Feldern der Objekttabelle:
  - `SUBTITLE`
  - `PATH`
  - `HTTP`

  Diese drei Felder haben den Typ A (Character) und eine Länge von 512 bzw. 1024 Zeichen. Damit diese Länge nicht verkleinert werden muß, könnte der Datentyp auf M (Text) geändert werden. Beim Feld HTTP ist das jedoch problematisch, da auf diesem Feld ein Index liegt, und im Microsoft SQL Server Indizes auf Textattributen nicht erlaubt sind. Daher wird für den Microsoft SQL Server das HTTP-Attribut mit maximal 255 Zeichen eingetragen, weil es vorrangig ist, einen Index für dieses Feld zu haben, und die Länge von 255 Zeichen für die HTTP-Adresse selten erreicht wird.
- Für den Microsoft SQL Server 7.0 gelten die o. g. Einschränkungen nicht. Allerdings dürfen indizierte Felder nicht mehr als 900 Zeichen enthalten. Daher müssen die beiden indizierten Felder
  - `PATH`
  - `HTTP`

  entsprechend auf 900 Zeichen begrenzt werden.
- Für Oracle Version 8 gilt folgendes: Die maximale Länge der indizierten Felder hängt von dem Parameter `db_block_size` ab, der nur beim Anlegen einer Datenbank in der Initialisierungsdatei festgelegt werden kann. Wenn der Parameter auf 1024 gesetzt wird, sind die beiden indizierten Felder

- PATH
- HTTP

auf 758 Zeichen begrenzt. Es wird empfohlen, den Wert auf 4096 bzw. 8192 zu setzen.

- Für DB2 gilt: Die Standardeinstellung des HTTP-Attributs von 1024 Zeichen muß auf maximal 255 Zeichen begrenzt werden.

Schritt 6: Alle VIP-Server starten

Nachdem die beschriebenen Konfigurationsänderungen an allen VIP-Servern durchgeführt worden sind, müssen alle Server neu gestartet werden.

Schritt 7: Website anlegen

Nach dem Starten der Server, melden Sie sich im VIP-Administrationssystem an und legen eine neue Website an. Alle neuen Websites werden entsprechend der geänderten Konfiguration automatisch mit Datenbankanbindung angelegt. Nach dem ersten Einrichten der Datenbankanbindung empfiehlt es sich als Vorsichtsmaßnahme, zunächst eine Test-Website anzulegen und damit zu arbeiten. Erst nachdem Sie verifiziert haben, daß das System richtig konfiguriert ist und alle Systemkomponenten einwandfrei funktionieren, sollten Sie mit dem Anlegen von Websites für den produktiven Betrieb beginnen.

> **Hinweis:** Bitte beachten Sie die im Abschnitt “Wichtige Hinweise:” auf Seite 89 angegebenen Konventionen hinsichtlich des Website-Namens.

Wenn es einmal während des Betriebs zu einem Abbruch der Verbindung zur Datenbank kommen sollte, werden der Pflege- und der QS-Server automatisch heruntergefahren. Der Produktions- und Administrationsserver laufen dagegen weiter. Zur Wiederherstellung der Datenbankverbindung müssen in diesem Fall jedoch nicht nur der Pflege- und QS-Server, sondern *auch* der Produktionsserver neu gestartet werden, wenn dieser auf das Datenbanksystem zugreift.

Einrichten von JDBC- bzw. JDBC-ODBC-Datenquellen

Für JDBC-ODBC-Datenquellen muß ein datenbankspezifischer ODBC-Treiber installiert sein. Wenn die Edit-, QS- und Produktionssysteme auf unterschiedliche Computer verteilt sind, muß die ODBC-Datenquelle auf jedem Host-Computer verteilt sein.

Hinweise:

Der Microsoft SQL Server darf nur im Zusammenhang mit nativen JDBC-Treibern verwendet werden. Er darf *nicht* über die JDBC-ODBC-Bridge betrieben werden.

Die Protokollierung der SQL-Schnittstellen sollte in der ODBC-Einstellung deaktiviert bzw. nur in begründeten Fällen und nicht unter Produktivbedingungen eingeschaltet werden, da das Logging die Performance stark beeinträchtigt.

Öffnen Sie die ODBC-Konfiguration *in der Windows-Systemsteuerung*, und fügen Sie eine VIP-Datenquelle als System-DSN hinzu:

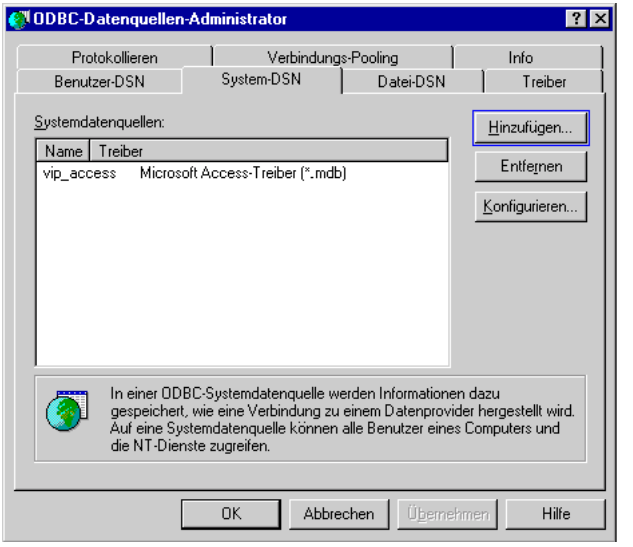

Abb. 16 – Einrichten einer ODBC-Systemdatenquelle

Jede ODBC-Datenquelle muß einen Namen haben. Um Probleme zu vermeiden, sollten Sie für diese Namen nur die Basisbuchstaben A-Z, a-z, Ziffern und Unterstriche (_) verwenden. Der Datenquellenname muß (wie auf Seite “DBC-Parameter” auf Seite 98 beschrieben) zusammen mit dem Präfix `JDBC:ODBC:` in der Serverkonfiguration eingetragen werden, und zwar als Wert des Parameters `DBCDATASOURCE` in der Datei **websites.properties**.

Die weitere Konfiguration ist abhängig vom verwendeten Datenbanksystem.

Oracle 8

Der Oracle-Server ist als Administrator zu installieren und zu konfigurieren (diese Beschreibung ist nur ein Beispiel für eine Installation, von der durchaus abgewichen werden kann). Die Standard-Benutzernamen und -Kennwörter sind: INTERNAL [ORACLE], SYS [CHANGE_ON_INSTALL], SYSTEM [MANAGER], SCOTT [TIGER], DEMO [DEMO] und DBSNMP [DBSNMP]. Für den Zugriff kann die erste Kennung (INTERNAL) benutzt werden. Um eine Oracle-Datenbank zu nutzen, gehen Sie wie folgt vor:

1. Starten Sie den Oracle Enterprise Manager. Beim Einloggen darf kein Dienstname angegeben werden, Sie müssen aber einen neuen Knoten mit dem Computernamen einrichten.
2. Im Storage Manager müssen Sie neuen Tablespace mit beliebigem Namen (z. B. “vip_db”) einrichten, wobei eine Größe von 25 MB ausreichend ist.
3. Im Security Manager müssen Sie einen neuen Benutzer mit beliebigem Namen einrichten (z. B. “vip_login”). Das Kennwort wird später in der VIP-Konfiguration benötigt. Als Tablespaces geben Sie den zuvor eingerichteten Tablespace “vip_db” und “TEMPORARY_DATA” an. Die Berechtigungen müssen mindestens CONNECT und DBA sein.
4. Als User-ID ist der zuvor im Security Manager eingerichtete Benutzer zu wählen.
5. Die Parameter `DBCUSER` und `DBCPASSWORD` in der Datei **websites.properties** erhalten als Wert den zuvor eingerichteten Login und das entsprechende Paßwort.

Die Parameter DBCDATASOURCE und DBCPARAMETER haben für Oracle-Datenbanken die folgenden Werte:

```
DBCDATASOURCE = jdbc:oracle:thin:@{host}:{port}:{dbmsname}
```

```
DBCPARAMETER = oracle.jdbc.driver.OracleDriver
```

host, port und dbmsname sind Platzhalter für konkrete Werte. dbmsname ist bei einer Standardinstallation “ORCL”.

6. Der in DBCPARAMETER einzutragende native, von Oracle gelieferte JDBC-Treiber ist oracle.jdbc.driver.OracleDriver.
7. Kopieren Sie den Oracle-Treiber in die **java**-Verzeichnisse des Edit-, QS- und Produktionssytems. Verwenden Sie als Oracle-Treiber den aktuellen thin-Treiber.
8. Öffnen Sie die Datei **startvip.bat** (Windows NT) bzw. **start.sh** (Unix) und ergänzen Sie die folgende Zeile um den Dateinamen des Treibers:

```
SET vip=.\java;.\java\vipserver.jar;.\java\{JDBC-Treiber}
```

9. Generieren Sie mit dem Programm Net8 Easy Config einen Net-Service-Namen.

DB2

Der DB2-Server ist als Administrator zu installieren und zu konfigurieren (diese Beschreibung ist nur ein Beispiel für eine Installation, von der durchaus abgewichen werden kann). Um eine DB2-Datenbank zu nutzen, gehen Sie wie folgt vor:

1. Richten Sie mit Hilfe der DB2 Steuerzentrale eine neue *Datenbank* mit beliebigem Namen (z. B. “vip_db”) ein. Geben Sie unter *Aliasname* ebenfalls einen beliebigen Namen ein.
2. Legen Sie desweiteren einen *Pufferpool* mit einer Seitengröße von mindestens 8 KB, besser 16 KB an. Anschließend muß die Datenbank neu gestartet werden.
3. Richten Sie einen *Tabellenbereich* ein, und geben Sie als Namen den Datenbankbenutzer an, unter dem das VIP-System auf die Datenbank zugreift.

Weiterhin ist der Name des Pufferpools sowie die Seitengröße anzugeben, die identisch mit der für den Pufferpool angegebenen Seitengröße sein muß. Geben Sie anschließend einen *Behälter* mit beliebigem Namen an.

4. Richten Sie einen Benutzer mit den Rechten *Datenbank verbinden* und *Tabellen erstellen* ein. Auch die Zugriffsrechte auf den zuvor eingerichteten Tabellenbereich müssen an diesen Benutzer vergeben werden.
5. Das Arbeiten mit CLOBs erfordert eine entsprechende Vergrößerung des *maximalen Zwischenspeichers für Anwendungssteuerung*. Diese Konfiguration kann mit Hilfe der DB2 Steuerzentrale vorgenommen werden.
6. Die Parameter `DBCUSER` und `DBCPASSWORD` in der Datei **`websites.properties`** erhalten als Wert den zuvor eingerichteten Benutzer und das entsprechende Paßwort.
7. Die Parameter `DBCDATASOURCE` und `DBCPARAMETER` haben für DB2-Datenbanken die folgenden Werte:

   ```
   DBCDATASOURCE = JDBC:db2://{host}:{port}/{aliasname}
   ```

   ```
   DBCPARAMETER = COM.ibm.db2.jdbc.net.DB2Driver
   ```

   `aliasname` ist ein Platzhalter für den beim Einrichten der Datenbank vergebenen Alias-Namen.

Microsoft SQL Server 6.5

Der Microsoft SQL Server ist als Administrator zu installieren und zu konfigurieren (diese Beschreibung ist nur ein Beispiel für eine Installation, von der durchaus abgewichen werden kann). Um eine Microsoft SQL Server-Datenbank zu nutzen, gehen Sie wie folgt vor:

1. Legen Sie ein neues *Database Device* mit beliebigem Namen für die VIP-Daten (z. B. “vip_dbdevice”) an. Die Größe sollte selbst für Testzwecke mindestens 30 MB betragen.
2. Legen Sie ein neues *Database Device* mit beliebigem Namen für die Temporär-DB (z. B. “vip_tempdbdevice”) an. Die Größe sollte auch für Testzwecke mindestens 50 MB betragen.

3. Richten Sie eine neue *Database* mit beliebigem Namen (z. B. “vip_db”) ein. Geben Sie “vip_dbdevice” als Database Device an, wobei Sie für den Datenbereich die gesamte Größe und für den Logbereich 0 MB angeben können.
4. Richten Sie ein neues *Login* mit beliebigem Namen (z. B. “vip_login”) ein. Das Kennwort wird später in der VIP-Konfiguration benötigt. Es müssen Zugriffsrechte für die Datenbanken “master”, “tempdb” und die zuvor eingerichtete Datenbank (“vip_db”) vergeben werden. Weiterhin ist als Default unbedingt das zuvor eingerichtete Database Device (“vip_dbdevice”) anzugeben.
5. Geben Sie dem zuvor eingerichteten Login (“vip_login”) der zuvor eingerichteten Datenbank (“vip_db”) und den Datenbanken “master” und “tempdb” alle Zugriffsrechte.
6. Die Datenbank “tempdb” muß in das zuvor eingerichtete Database Device (“vip_tempdbdevice”) erweitert werden, da die Standardeinstellung von 2 MB nicht ausreicht. Weiterhin ist für diese Datenbank die Option *Truncate on Checkpoint* einzuschalten.
7. Der Microsoft SQL Server darf nur mit einem nativen JDBC-Treiber betrieben werden. Informationen zur Installation des JDBC-Treibers sind den Angaben des jeweiligen Herstellers zu entnehmen.
8. Die Parameter `DBCUSER` und `DBCPASSWORD` in der Datei **`websites.properties`** erhalten als Wert das zuvor eingerichtete Login und das entsprechende Paßwort.

Microsoft SQL Server 7.0

Der Microsoft SQL Server ist als Administrator zu installieren und zu konfigurieren (diese Beschreibung ist nur ein Beispiel für eine Installation, von der durchaus abgewichen werden kann). Voraussetzung für die Installation ist, daß das Service Pack 1 des IE 4.01 installiert ist. In Version 7.0 des Microsoft SQL Servers sind folgende Schritte durchzuführen:

1. Bei der Auswahl der zu installierenden Module sollte alles bis auf die Entwicklungs-Tools angekreuzt werden. Die Volltextsuche wird nicht benötigt,

kann aber ebenfalls ausgewählt werden. Im weiteren Verlauf können die Standardeinstellungen übernommen werden.

2. Der Installationsablauf erfordert danach einen Neustart des Computers. Die Microsoft SQL Server-Dienste werden nach dem Neustart automatisch gestartet. Die unter Schritt 3 - 6 beschriebenen Einstellungen werden über den Enterprise Manager durchgeführt.
3. Legen Sie eine neue Datenbank an, z. B. “vip_db”, die eine Anfangsgröße von 20 MB aufweisen sollte. Als Wert für die automatische Vergrößerung sollte 10% angegeben werden. Die Größe der Datenbank sollte nicht eingeschränkt werden. Darüber hinaus müssen in der Protokolldatei ähnliche Parameter festgelegt werden.
4. Überprüfen Sie, ob für die bereits bestehende Datenbank “tempdb” eine automatische Vergrößerung von 10% eingestellt ist.
5. Unter dem Punkt *Sicherheit* muß ein neuer Benutzer (z. B. “vip_login”) mit einem Paßwort für die zuvor eingerichtete Datenbank angelegt werden. Es muß *System Administrator* als *Serverrolle* angekreuzt werden und Zugriff auf alle Datenbanken bis auf die Beispieldatenbank “Northwind” gewährt werden.
6. Die weiteren Konfigurationsschritte sind identisch mit denen des Microsoft SQL Servers Version 6.5 (ab Schritt 7).

Einstellung der Speicherstrategie (Verdrängung)

Die zu verwendende Speicherstrategie für die Objektspeicherung wird durch den System-Manager bestimmt. Es ist dabei zwischen der Speicherstrategie mit und ohne Verdrängung zu unterscheiden. In der Praxis sind folgende Konfigurationen sinnvoll:

- dateibasierte Datenhaltung – ohne Verdrängung
- datenbankbasierte Datenhaltung – mit Verdrängung

Speicherstrategie ohne Verdrängung

Im Falle der dateibasierten Datenhaltung (in CSV-Dateien) sollte der System-Manager ohne Verdrängung eingestellt werden. Dazu ist folgender Eintrag in die Konfigurationsdatei **websites.properties** aufzunehmen:

```
SM = de.gauss.vip98.server.systemmanager.VipFileSystemManager
```

Dieser Eintrag kann als Standardeinstellung (im allgemeinen Abschnitt) oder aber Website-spezifisch (in den einzelnen Website-Abschnitten) erfolgen.

Speicherstrategie mit Verdrängung

In der Regel wird die datenbankbasierte Datenhaltung für sehr große Websites (mit mehr als 10 000 Objekten) genutzt. Bei einer solchen Anzahl von Objekten wäre es sehr hauptspeicherintensiv, alle Objekte gleichzeitig im Speicher zu halten. Durch die Verdrängungsstrategie besteht die Möglichkeit, die Objektdaten auszulagern und immer erst zum Zeitpunkt des Zugriffs in den Speicher zu laden. Dies erfordert aber einen sehr schnellen Zugriff auf die Objektdaten, der nur durch ein Datenbanksystem gewährleistet werden kann.

Im Falle der datenbankbasierten Datenhaltung muß daher der System-Manager mit Verdrängung gewählt werden. Dazu ist folgender Eintrag in die Konfigurationsdatei **websites.properties** aufzunehmen:

```
SM = de.gauss.vip98.server.systemmanager.VipDBSystemManager
```

Der DB-System-Manager hält die VIP-Objekte nicht alle im Hauptspeicher, sondern verdrängt sie nach der folgenden Strategie aus dem Hauptspeicher:

VIP-Objekte können vollständig geladen sein. Sie sind dann im Cache gespeichert. Wird ein VIP-Objekt benötigt, das nicht im Cache vorhanden ist, wird es aus der Datenbank geladen.

Die folgende Abbildung zeigt das Verdrängen und das Nachladen von Objekten:

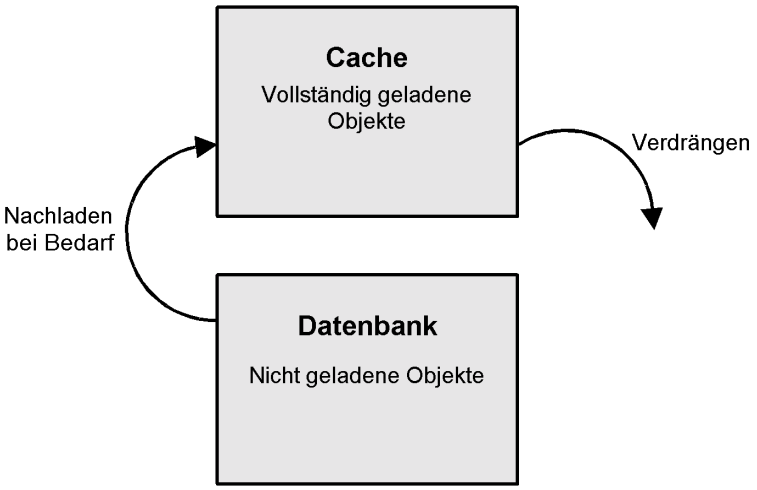

Abb. 17 – Speicherstrategie mit Verdrängung

Durch zwei weitere Angaben in der Konfigurationsdatei **websites.properties** wird die Größe des Caches und der Chunk-Size eingestellt, die bei der Verdrängung genutzt werden:

```
SM =            de.gauss.vip98.server.systemmanager.VipDBSystemManager
FIRST_CACHE =   10000
CHUNK_SIZE =    2000
```

`FIRST_CACHE` gibt an, wie viele Objekte beim Starten des VIP-Servers gleichzeitig im Cache enthalten sein können. Mit der Angabe `CHUNK_SIZE` wird die Anzahl der Objekte festgelegt, um die der Cache vergrößert wird, wenn eine Operation mehr Objekte im geladenen Zustand erfordert als zu diesem Zeitpunkt im Cache gehalten werden können und kein Objekt verdrängt werden kann.

4.7 Datensicherung

Aus Sicherheitsgründen sollten die Datenbestände des VIP-Systems in regelmäßigen Abständen archiviert werden. Um eine Datensicherung (Backup) durchzuführen, muß die Konsistenz des Datenbestandes gewährleistet sein, d. h. wenn die Daten eines VIP-Servers gesichert werden, dürfen keine Aktionen innerhalb dieses Servers stattfinden. Zu diesem Zweck steht der Runlevel “Backup” zur Verfügung (weitere Informationen über Runlevels finden Sie im Abschnitt 5.6 “Systemadministration” auf Seite 154).

Der Runlevel “Backup” ermöglicht die Durchführung einer Datensicherung, ohne daß ein Beenden der VIP-Server erforderlich ist. Die betreffenden Server werden während des Sicherungsvorgangs in einen kontrollierten und reversiblen Haltezustand versetzt.

> **Hinweis:** Die eigentliche Datensicherungsoperation kann nicht vom VIP-System ausgeführt werden, sondern muß mit einem externen Programm vorgenommen werden.

Sobald sämtliche Daten aller betreffenden VIP-Server gesichert sind, wird der Runlevel auf allen Servern wieder freigegeben, und das VIP-System ist wieder betriebsbereit.

Durchführung der Datensicherung

Die Durchführung der Datensicherung erfolgt in mehreren Schritten:

- Starten des externen Backup-Programms
- Herunterfahren der VIP-Server in den Runlevel “Backup”
- Sichern des Datenbestandes (Dateien und Datenbanktabellen)
- Aufheben des Runlevels “Backup” für die VIP-Server

Schritt 1 – Starten des externen Backup-Programms

Starten Sie das externe Programm, das die eigentliche Datensicherung vornehmen soll.

Schritt 2 – Herunterfahren der VIP-Server in den Runlevel “Backup”

Bevor der Datenbestand des VIP-Systems gesichert werden kann, muß der Runlevel “Backup” bei den entsprechenden VIP-Servern reserviert werden. Rufen Sie zu diesem Zweck das Skript **vip_backup.bat** (Windows NT) bzw. **vip_backup.sh** (Unix) auf, das sich im Verzeichnis **{VIP-Installationsverzeichnis}\admin** befindet.

Das externe Backup-Programm sollte idealerweise so konfiguriert werden, daß die Datei **vip_backup.bat** bzw. **vip_backup.sh** selbständig aufgerufen wird.

Im folgenden wird der Aufruf der Batch-Datei dargestellt. Er erfordert zusätzlich die Angabe bestimmter Parameter, die anschließend erläutert werden.

```
vip_backup.bat {vip_login} {vip_password} {server_list} ⇨
  [{user_info_message}] [{verbose_setting}]
```

Die Aufrufparameter sind in der dargestellten Reihenfolge einzugeben. Sie haben folgende Bedeutung:

`{vip_login}`	Kennung des Adminbenutzers im VIP-System
`{vip_password}`	Paßwort des Adminbenutzers im VIP-System
`{server_list}`	Angabe der VIP-Server, für die der Runlevel “Backup” reserviert werden soll. **Hinweis:** Werden mehrere Server angegeben, müssen diese in Anführungszeichen aufgeführt und die einzelnen Servernamen durch Kommata getrennt werden. Dabei dürfen keine Leerzeichen eingefügt werden. Folgende Angaben sind erlaubt: `ADMIN,EDIT,QS,PROD`.

Desweiteren sind optionale Angaben möglich, die im folgenden erläutert werden.

`[{user_info_message}]`	Angabe einer Meldung, die erscheint, sobald versucht wird, eine den Datenbestand verändernde Aktion auf einem VIP-Server durchzuführen, der sich im Runlevel “Backup” befindet. Bei einer Meldung, die aus mehr als einem Wort besteht, ist die Angabe in Anführungszeichen zu setzen. Erfolgt keine Angabe, wird folgende Standardmeldung angezeigt: “Aktion zur Zeit nicht möglich, da ein Backup auf diesem Server läuft.”
`[{verbose_setting}]`	Angabe, ob erweiterte Informationsmeldungen angezeigt werden sollen. Standardmäßig ist dieser Parameter ausgeschaltet. Erlaubt sind die Angaben `YES` und `NO`.

Nach dem Aufruf des Skripts mit der Angabe aller erforderlichen Parameter werden die entsprechenden VIP-Server in den Runlevel “Backup” heruntergefahren. Dieser Prozeß wird automatisch durch das Administrationssystem übernommen.

Schritt 3 – Sichern des Datenbestandes (Dateien und Datenbanktabellen)

Die Sicherung des Datenbestandes erfolgt, wenn die entsprechenden VIP-Server in den Runlevel “Backup” versetzt worden sind.

Sobald sich ein VIP-Server in diesem Runlevel befindet, wird der Zustand durch die generierte Flag-Datei **`backup.vip`** angezeigt. Diese Datei befindet sich im Verzeichnis des jeweiligen Servers, also z. B. im Verzeichnis **`{VIP-Installationsverzeichnis}\edit`**. Dementsprechend wird für jeden Server eine Flag-Datei generiert.

Die Flag-Datei enthält Informationen darüber, wann der entsprechende VIP-Server in den Runlevel “Backup” versetzt worden ist, und zwar in Form einer Datums- und Uhrzeitangabe. Aus diesen Angaben können allerdings keine Rückschlüsse gezogen werden, ob bzw. seit wann der eigentliche Prozeß der Datensicherung bereits stattfindet.

Schritt 4 – Aufheben des Runlevels “Backup” für die VIP-Server

Ein VIP-Server befindet sich so lange im Runlevel “Backup”, wie die Flag-Datei existiert. Damit der Runlevel für den entsprechenden VIP-Server nach erfolgreicher Datensicherung wieder aufgehoben werden kann, muß die Flag-Datei gelöscht werden. Idealerweise erfolgt dies automatisch durch das Backup-Programm, das zu diesem Zweck ein entsprechendes Skript beinhalten muß.

Nach dem Löschen der entsprechenden Flag-Dateien sind die VIP-Server wieder betriebsbereit.

Verhalten im Fehlerfall

Sollten Fehler während des Datensicherungsprozesses auftreten, werden diese nicht durch das VIP-System ausgewertet. Verantwortlich für die erfolgreiche Durchführung der Datensicherung ist der Systemadministrator.

Wenn bei einem VIP-Server die Flag-Datei **backup.vip** durch das externe Backup-Programm nicht gelöscht werden kann, verbleiben alle betreffenden VIP-Server im Runlevel “Backup”. Der Systemadministrator muß also sicherstellen, daß sämtliche Flag-Dateien nach vollendeter Datensicherung wieder gelöscht werden bzw. daß der Runlevel “Backup” für alle VIP-Server wieder aufgehoben wird. Gegebenenfalls müssen die Flag-Dateien manuell gelöscht werden, damit die VIP-Server wieder betriebsbereit sind.

Wiederherstellung eines früheren Datenbestands

Bevor ein früherer Datenbestand aus den Backup-Dateien wiederhergestellt werden kann, müssen die Server heruntergefahren werden. Nach dem Herunterfahren der Server müssen alle Dateien in den Verzeichnissen

{VIP-Installationsverzeichnis}\{Servername}\{Website-Name}

sowohl für den Edit-, QS- und Produktionsserver als auch für jede Website durch die entsprechenden Dateien aus der Sicherungskopie ersetzt werden.

Wenn Sie mit einer Datenbank arbeiten, müssen Sie auch die Tabellen durch die Tabellen aus dem Backup austauschen.

Darüber hinaus müssen die Dateien im Verzeichnis

{VIP-Installationsverzeichnis}\admin\UserAdmin

durch die entsprechenden Dateien der Sicherungskopie ersetzt werden.

Anschließend können Sie – nach dem erneuten Hochfahren der VIP-Server – mit dem VIP-System weiterarbeiten, das dann den Status der eingespielten Sicherungskopie widerspiegelt.

4.8 Konfiguration des SetExecutable-Agent

Das Einbinden von beliebigen Dateien war bereits in früheren VIP-Versionen mit Hilfe des Objekttyps “Sonstige” möglich. Das Besondere an dem neuen Objekttyp “CGI Skript” ist, daß auf Unix-Systemen das sogenannte “Executable Bit” gesetzt wird. Bei Objekten des Typs “Sonstige” ist das nicht der Fall. Das “Executable Bit” sorgt dafür, daß die Datei durch ein Programm, etwa den HTTP-Server, aufgerufen und auch ausgeführt werden kann.

Im Zusammenhang mit den Aktionen des VIP-Workflows (Vorlegen, Freigeben usw.) werden die Daten eines Objekts zwischen den VIP-Servern hin und her kopiert. Aus technischen Gründen würden solche Aktionen dazu führen, daß das Objekt sein gesetztes “Executable Bit” verliert. Um zu gewährleisten, daß das “Executable Bit” eines CGI-Objekts erhalten bleibt, bietet VIP einen speziellen Server-Agenten (SetExecutable-Agent). Wenn Ihr VIP-System unter Unix läuft, müssen Sie für jeden der entsprechenden Server diesen Agenten einbinden. Dazu fügen Sie den folgenden Eintrag in die Datei

{VIP-Server}\config\serverAgents.properties ein:

```
de.gauss.vip98.user.makeexecutable.SetExecutableAgent:CGI
```

Danach müssen Sie die VIP-Server neu starten.

4.9 DiskSpace-Agent

Der DiskSpace-Agent überprüft in definierbaren Zeitintervallen den verbleibenden Festplattenspeicherplatz und sendet rechtzeitig Benachrichtigungen an vorher festgelegte Personen, z. B. an die Systemadministratoren, wenn der verbleibende Speicherplatz einen festgelegten Wert unterschritten hat. Im Extremfall fährt der Agent das Pflege- und QS-System herunter, um sicherzustellen, daß keine Daten durch mangelnden Speicherplatz verlorengehen.

Hinweis: Auch der Einsatz dieses Agenten kann keinen hundertprozentigen Schutz vor speicherplatzbedingten Fehlern bieten. Der Agent ist aber so konzipiert, daß dieses Risiko bei richtiger Anwendung auf ein Minimum reduziert wird. Er soll die Systemadministratoren bei ihrer Arbeit unterstützen. Dennoch sollte nie auf das Erstellen regelmäßiger Backups verzichtet werden. Generell wird der Einsatz eines professionellen Überwachungssystems empfohlen.

Einsatz des DiskSpace-Agenten

Der Agent kann in den Pflege-, QS- und Produktionsserver eingebunden werden. Dazu muß in der Datei **{VIP-Installationsverzeichnis}\{Server}\config\serverAgents.properties** für den Pflege-, QS- und Produktionsserver folgender Eintrag vorgenommen werden:

```
de.gauss.vip98.user.diskSpaceAgent.DiskSpaceAgent:
```

Die folgende Abbildung zeigt eine Beispielkonfiguration, bei der alle Systeme auf einem Rechner installiert sind und der DiskSpace-Agent in den Pflegeserver eingebunden wurde.

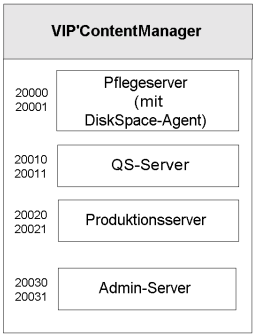

Abb. 18 – Beispielkonfiguration mit DiskSpace-Agenten auf dem Pflegeserver

Bei verteilten Systemen, d. h. wenn sich alle Server auf separaten Rechnern befinden, sollte der Agent so eingesetzt werden, daß für jeden Rechner ein eigener Agent zur Verfügung steht.

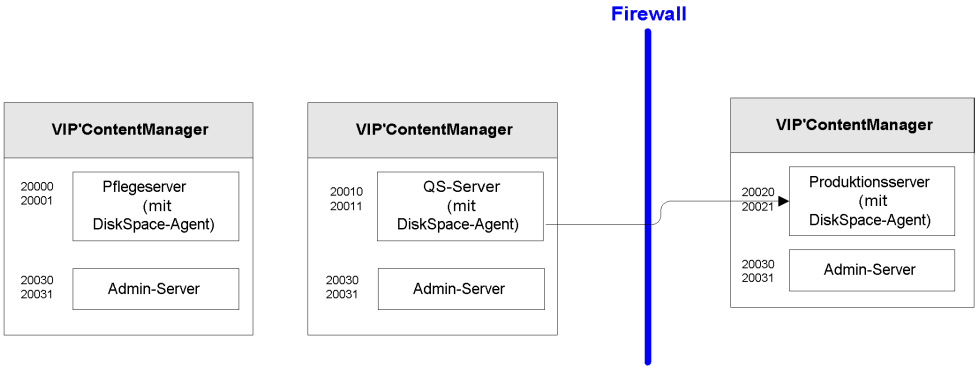

Abb. 19 – Konfiguration der Server auf verschiedenen Rechnern

Bei einer Systemkonfiguration mit separatem Produktionssystem muß jeweils ein Agent im separaten Produktionssystem und im Pflegesystem zum Einsatz kommen. Die Agenten können alternativ auch ins Administrations- oder Qualitätssicherungssystem eingebunden werden. Sie brauchen in diesem Fall jedoch nicht mehrere Agenten in den zuletzt genannten Systemen einzusetzen, da sonst zwei Agenten denselben Festplattenplatz überwachen.

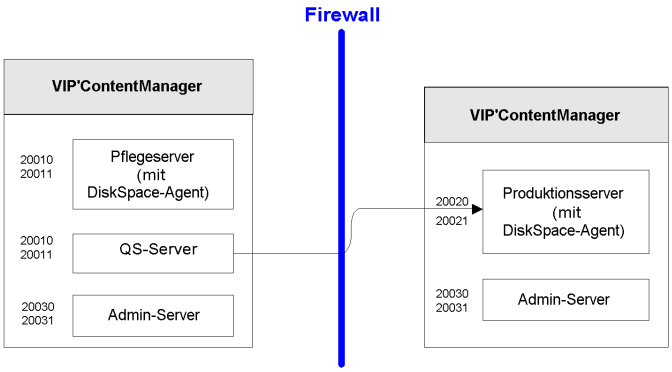

Abb. 20 – Konfiguration der Systeme mit separatem Produktionsserver

Hinweis: Beachten Sie bitte, daß Sie den Server nach den vorgenommenen Eintragungen erneut starten müssen, damit die Einstellungen wirksam werden.

Konfiguration des DiskSpace-Agenten

Damit der Agent seine Aufgabe erfüllen kann, müssen zunächst einige Einstellungen in der Konfigurationsdatei

{VIP-Installationsverzeichns}\{Server}\config\viptools\diskSpaceAgent\diskSpace.properties

vorgenommen werden. Die dabei für den Benutzer relevanten Bereiche gliedern sich in eine Default-Section und mehrere Threshold-Sections, die im folgenden auszugsweise dargestellt werden:

```
...
mailto=
debugmode=off
sleepingtime=2
timetype=h
startingtest=on
...
```

```
...
[threshold1]
action=mail
sleepingtime=1
threshold=200

[threshold2]
action=mail
threshold=150

[threshold3]
action=mail
threshold=100

[threshold4]
action=mail,shutdown
threshold=50
...
```

Im folgenden werden die einzelnen Attribute beschrieben, die zum Arbeiten mit dem DiskSpace-Agenten definiert werden müssen bzw. können. Zur Verdeutlichung finden Sie jeweils einen Beispieleintrag im Anschluß an die Beschreibung.

- `mailto`: Damit der Agent gestartet werden kann, muß zumindest das Attribut `mailto` in der Default-Section (und gegebenenfalls zusätzlich in den Threshold-Sections) der Konfigurationsdatei angepaßt werden. Hier werden die Mailadressen aller Personen (durch Kommata abgetrennt) eingetragen, die eine Benachrichtigung über den Status des DiskSpace-Agenten erhalten sollen. Wird das Attribut in einer Threshold-Section festgelegt, wird bei Erreichen der in dieser Section angegebenen Speichergrenze zusätzlich eine E-Mail an die eingetragenen Adressen geschickt. Bitte beachten Sie, daß dieser Eintrag in einer Zeile, d. h. ohne Zeilenumbruch eingegeben werden muß.

```
mailto=hugo@myDomain.com, hans@myDomain.com
```

- `debugmode`: Hier kann der Testmodus ein- bzw. ausgeschaltet werden.

```
debugmode=off
```

- `sleepingtime`: Dieses Attribut gibt die Zeitspanne an, die zwischen zwei Überprüfungen durch den DiskSpace-Agenten liegt, und kann sowohl in der Default- als auch in den Threshold-Sections eingetragen werden. Die Einheit der Zeitspanne wird durch das folgende Attribut `timetype` definiert. Der in der Default-Section gesetzte Wert gilt als Startwert. Wenn eine in einer Threshold-Section definierte Speichergrenze erreicht wird und in dieser Threshold-Section das Attribut ebenfalls gesetzt ist, gilt der neue Wert.

```
sleepingtime=3
```

- `timetype`: Die Einheit der Zeitspanne `sleepingtime`. Mögliche Werte sind: `m` (Minuten) oder `h` (Stunden). Dieser Eintrag kann nur in der Default-Section der Konfigurationsdatei vorgenomen werden.

```
timetype=h
```

- `startingtest`: Hier kann festgelegt werden, ob direkt nach dem Start des Agenten eine E-Mail an alle in der Default-Section durch das Attribut `mailto` definierten Empfänger geschickt wird, um zu überprüfen, ob der Agent fehlerfrei arbeitet.

```
startingtest=on
```

- `threshold`: Mit diesem Attribut, das in jeder Section festgelegt werden muß, wird eine Speichergrenze (in MB) definiert, ab der eine entsprechende Aktion (Verschicken einer E-Mail oder Herunterfahren des Pflege- oder QS-Systems) ausgelöst wird. Im obigen Beispiel sind vier kritische Speichergrenzen angegeben, d. h. der DiskSpace-Agent wird ausgelöst, wenn der verfügbare Speicherplatz unter 200, 150, 100 und 50 MB fällt.

Hinweis: Bitte beachten Sie, daß die Section `[threshold1]` einen größeren Wert für `threshold` besitzen muß als `[threshold2]`, die Section `[threshold2]` einen größeren Wert für `threshold` haben muß als `[threshold3]` usw., da dies der Reihenfolge entspricht, in der die Speichergrenzen überschritten werden. Standardmäßig sind hier schon sinnvolle Werte voreingestellt. Es empfiehlt sich, hier nur dann größere Werte festzulegen, wenn große Websites (mit mehr als 10 000 Objekten) von den VIP-Servern verwaltet werden. Außerdem sollten Sie hier mit größeren Werten arbeiten, wenn noch andere Programme, die Speicherplatz dynamisch belegen, auf den Partitionen installiert sind, auf denen sich die VIP-Server befinden.

```
[threshold1]
...
threshold=200

[threshold2]
...
threshold=150

[threshold3]
...
threshold=100

[threshold4]
...
threshold=50
```

- `action`: Hier werden die Aktionen angegeben, die beim Erreichen der kritischen Speichergrenze ausgelöst werden sollen. Mögliche Werte sind: `mail` (das Verschicken einer E-Mail), `shutdown` (das Herunterfahren des Pflege- und QS-Systems). Diese Werte sind in einer kommaseparierten Liste anzugeben.

```
action=mail,shutdown
```

4.10 Einstellen der Hauptspeicheranforderung

Bei großen Websites sollten Sie in der Startdatei **startvip.bat** bzw. **start.sh** den Parameter `-mx` vergrößern, um Fehlermeldungen bzw. Fehlfunktionen des VIP-Clients vorzubeugen. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie die Datei **startvip.bat** bzw. **start.sh**.
2. Setzen Sie den Parameter `-mx` in der Zeile

   ```
   START /MIN "{Servername} 5e" java -ms64m -mx256m
   de.gauss.vip98.server.VIPServer
   ```

   bzw.

   ```
   java -mx256m de.gauss.vip98.server.VIPServer -warning &
   ```

   für alle vier Server auf einen entsprechend höheren Wert, z. B. `-mx512m`.

KAPITEL 5

Arbeiten im Administrationssystem

Im Administrationssystem des VIP'ContentManager wird sowohl die Verwaltung von Websites und Servern, als auch die Administration von Benutzern sowie Benutzergruppen und -rollen durchgeführt. Der Zugang zu diesen administrativen Funktionen ist nur über das Administrationssystem möglich.

Das Administrationssystem wird von der VIP-Startseite aus aufgerufen und präsentiert sich dann als Fenster mit mehreren Registern (auch Panels genannt). Auf diesen sind die Funktionen des Systems verfügbar.

Das Anmelden im Administrationssystem ist zur Zeit nur dem Benutzer "admin" erlaubt, wobei das Anfangspaßwort nach der Installation standardmäßig "admin" ist. Um die Sicherheit Ihres Systems zu schützen, muß ein geeignetes Paßwort für den Benutzer "admin" eingestellt und regelmäßig geändert werden.

Neben den hier beschriebenen Aufgaben der Systemadministration gibt es eine Reihe von Funktionen, die in anderen Bereichen (zum Beispiel im Pflegesystem) durchzuführen sind, wie die Funktionen der Zugriffskontrolle (siehe Kapitel 6 "Zugriffskontrolle"). Da diese Funktionen zum Teil einen administrativen Charakter haben, werden sie an anderer Stelle in diesem Handbuch beschrieben.

5.1 Anmelden im Administrationssystem

Wenn Sie auf den VIP'ContentManager zugreifen möchten, starten Sie Ihren Webbrowser und öffnen die Startseite des VIP'ContentManager. Wenn Sie die HTTP-Adresse der Startseite nicht kennen, wenden Sie sich an Ihren Systemadministrator.

Die Startseite des VIP'ContentManager enthält jeweils einen Link auf das Pflege-, QS- und das Administrationssystem.

Abb. 21 – Die Startseite des VIP-Systems

Klicken Sie auf das Symbol *Admin*, um das Administrationssystem zu starten. Es erscheint folgender Anmeldedialog:

Abb. 22 – Anmeldedialog für das Administrationssystem

Geben Sie die Benutzerkennung “admin” und das entsprechende Paßwort ein. (Das Anfangspaßwort nach der Installation lautet ebenfalls “admin”.)

> **Hinweis:** Beachten Sie bitte, daß die Groß- und Kleinschreibung in der Benutzerkennung sowie im Paßwort unterschieden wird. Der Benutzer “admin” kann sich also nicht mit “Admin” oder “ADMIN” anmelden, da der VIP’ContentManager von drei unterschiedlichen Benutzern ausgehen würde.

Wenn Sie sich erfolgreich am System angemeldet haben, erscheint ein Fenster mit mehreren Panels. Mit Hilfe der einzelnen Panels können Sie Ihr System administrieren, d. h. im einzelnen:

- *Website-Administration:* Anlegen und Einrichten von Websites, dabei Zuordnen von Website-Administratoren, von Benutzern, Gruppen und Rollen.
- *Benutzer-Administration:* Anlegen und Einrichten von neuen Benutzern sowie Änderung von Benutzereinstellungen, Zuordnen von Benutzern zu Gruppen und Rollen, Festlegen weiterer Eigenschaften wie Stellvertreter, E-Mail-Adressen, Funktionsbereiche und Standardzugriffsrechte.
- *Gruppen-Administration:* Anlegen und Einrichten von neuen Gruppen sowie Änderung von Gruppeneinstellungen, Zuordnen von Benutzern zu einer Gruppe, Festlegen weiterer Eigenschaften wie Standardzugriffsrechte.

- *Rollen-Administration:* Anlegen und Einrichten von neuen Rollen sowie Änderung von Rolleneinstellungen, Zuordnen von Benutzern zu einer Rolle, Festlegen weiterer Eigenschaften wie Standardzugriffsrechte.
- *Systemadministration:* Anhalten der VIP-Server.
- *LDAP:* Übernahme von Daten aus einem Verzeichnisdienst, Abgleich mit den aktuellen Daten des Verzeichnisdienstes.

In allen Zuordnungsdialogen des Administrationsfensters gibt es den Button *Admin.Info.*, über den Sie den Dialog *Administrations Information* öffnen können. Dieser Dialog liefert Ihnen in übersichtlicher Form Informationen über die entsprechenden Zuordnungen von Websites, Benutzern, Gruppen und Rollen.

5.2 Website-Administration

Dieses Panel des Administrationsfensters dient der Website-Administration. Hier können Sie neue Websites anlegen und bestehende Websites löschen. Über die Buttons *Gruppen*, *Rollen* und *Benutzer* rufen Sie die entsprechenden Zuordnungsdialoge auf, um Gruppen, Rollen und Benutzer der ausgewählten Website zuzuordnen.

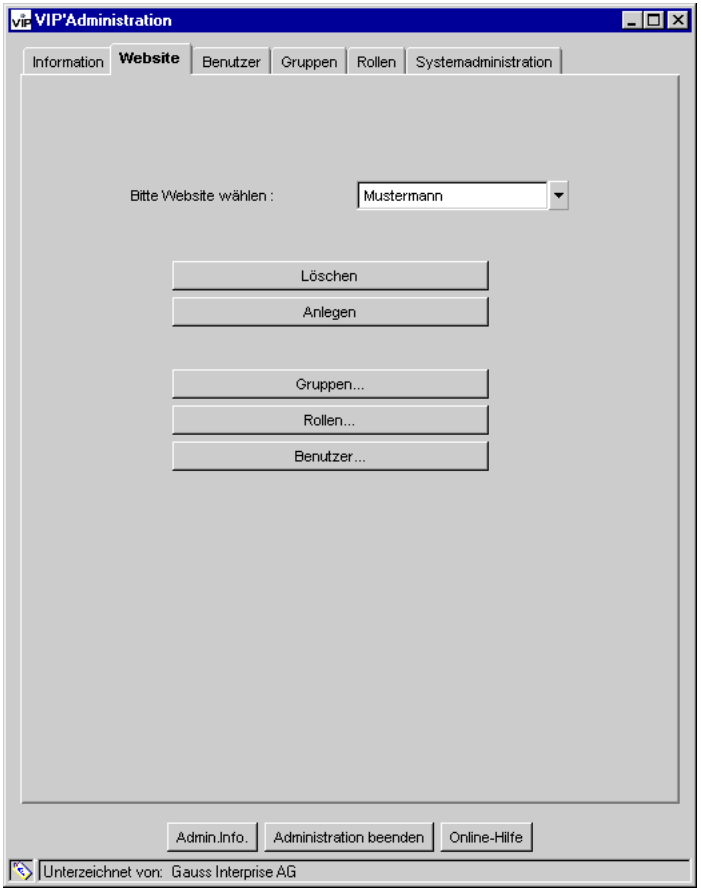

Abb. 23 – Panel der Website-Administration

Website anlegen

Um eine neue Website anzulegen, klicken Sie im Website-Panel des Administrationsfensters auf den Button *Anlegen*. Es erscheint ein Dialog, in dem Sie die Grundeinstellungen der Website angeben.

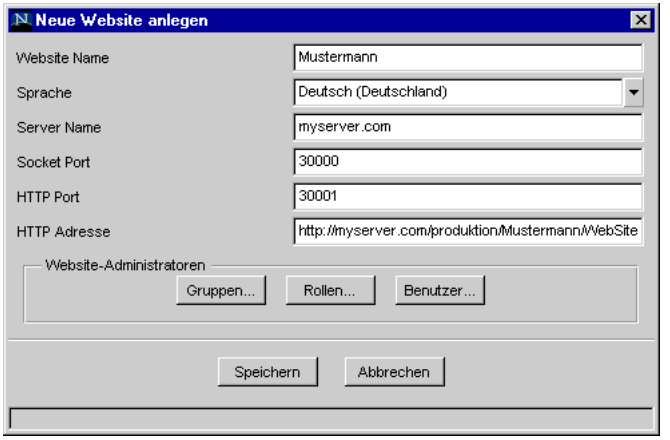

Abb. 24 – Dialog zum Anlegen einer neuen Website

Website-Name

Geben Sie hier den Namen für die neue Website ein.

Der Name einer Website darf nur folgende Zeichen enthalten:

- a-z, A-Z, 0-9, *keine* Umlaute bzw. “ß”

  Am *Anfang* eines Website-Namens dürfen die Ziffern 0-9 *nicht* verwendet werden!

Hinweis: Bitte beachten Sie, daß beim Anlegen einer Website die in früheren Versionen erlaubten Zeichen -(Bindestrich), _(Unterstrich) und .(Punkt) im Website-Namen ab der Version 5e.03 *nicht* mehr erlaubt sind. Bei Websites, die in einer früheren Version angelegt wurden und deren Namen die aufgeführten Zeichen enthalten, ist eine einwandfreie Funktionsweise jedoch gewährleistet.

Wenn sich das Produktionssystem einer Website auf dem gleichen Server wie das Pflege- und QS-System befindet und über die HTTP-Adresse

http://{server_name}/produktion/{website_name}/WebSite

aufgerufen werden kann, braucht beim Anlegen einer Website nur das Feld *Website Name* ausgefüllt zu werden.

Soll die Website im Produktionssystem über eine andere HTTP-Adresse angesprochen oder das Produktionssystem dieser Website auf einem anderen Server (physikalisch oder virtuell) eingerichtet werden, müssen in den übrigen Feldern der Servername des Produktionsservers, dessen Socket-Port, HTTP-Port sowie die vollständige HTTP-Adresse eingetragen werden.

Website-Administratoren

Im Dialog *Neue Website anlegen* können Sie über die Buttons *Benutzer*, *Gruppen* und *Rollen* jeweils einen weiteren Dialog aufrufen, in dem Sie die Website-Administratoren der neuen Website festlegen können.

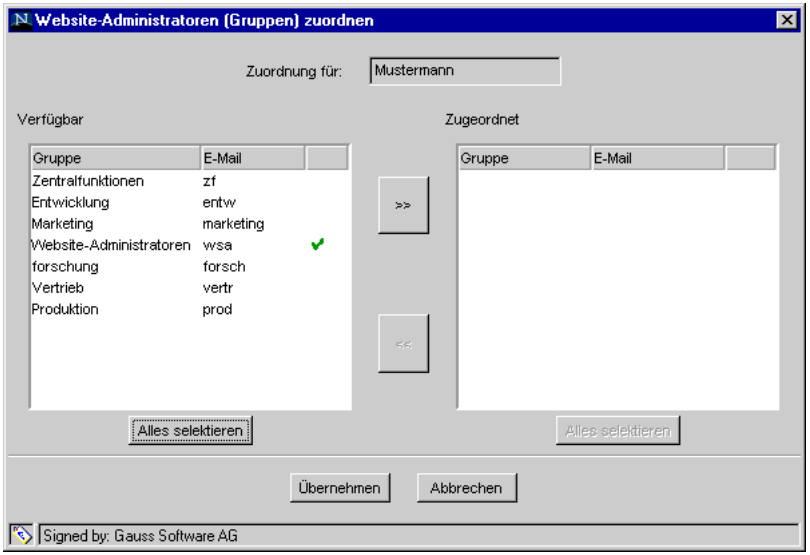

Abb. 25 – Zuordnung von Website-Administratoren

Die ausgewählten Benutzer, Gruppen oder Rollen haben uneingeschränkten Zugriff auf die Website, d. h. sie können auf der ersten Ebene der Website Themen anlegen, ändern und freigeben sowie Zugriffsrechte für diese Themen vergeben.

Wenn Sie keine Website-Administratoren für die Website festlegen, werden die Zugriffsrechte auf die Website automatisch folgendermaßen festgelegt:

- Der Benutzer “admin” ist Website-Administrator. Er hat uneingeschränkte Zugriffsrechte auf die Website und das Recht, die Zugriffsrechte zu ändern.
- Alle anderen Benutzer haben uneingeschränkte Zugriffsrechte auf die Website, bis auf das Recht, die Zugriffsrechte zu ändern und Baumoperationen durchzuführen. Dieses hat nur der Benutzer “admin”.

Zuordnung von Gruppen zu einer Website

Um einer Website neue Gruppen zuzuordnen oder die Gruppenzuordnung zu ändern, wählen Sie in der Website-Administration die gewünschte Website aus und rufen über den Button *Gruppen* den Gruppenzuordnungsdialog auf.

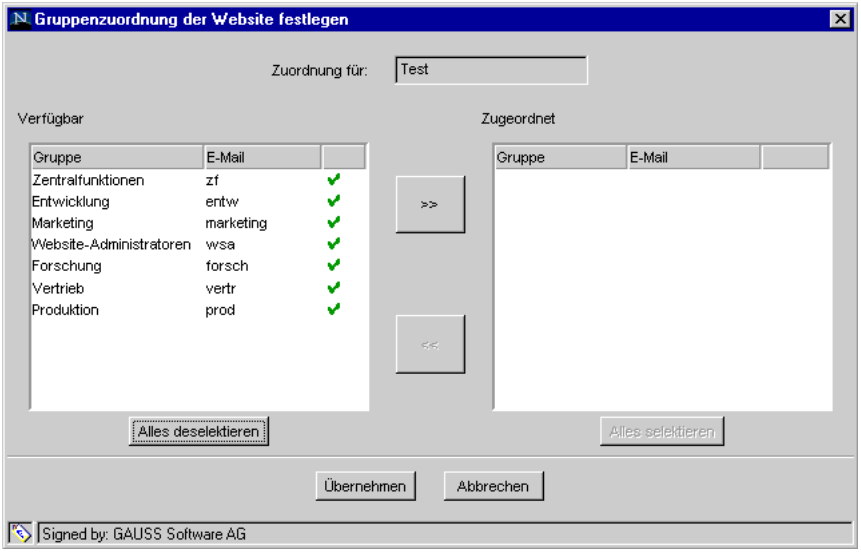

Abb. 26 – Dialog zur Zuordnung von Gruppen zu einer Website

Stellen Sie hier die gewünschte Gruppenzuordnung ein, und klicken Sie auf *Übernehmen*, um die Einstellung zu speichern.

Zuordnung von Rollen zu einer Website

Um einer Website neue Rollen zuzuordnen oder die Rollenzuordnung zu ändern, wählen Sie in der Website-Administration die gewünschte Website aus und rufen über den Button *Rollen* den Rollenzuordnungsdialog auf.

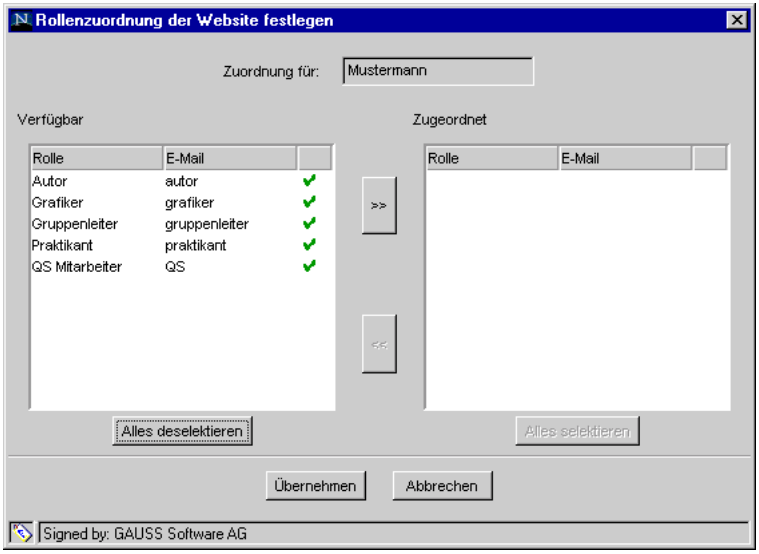

Abb. 27 – Dialog zur Zuordnung von Rollen zu einer Website

Stellen Sie hier die gewünschte Rollenzuordnung ein, und klicken Sie auf *Übernehmen*, um die Einstellung zu speichern.

Zuordnung von Benutzern zu einer Website

Um einer Website neue Benutzer zuzuordnen oder die Benutzerzuordnung zu ändern, wählen Sie in der Website-Administration die gewünschte Website aus und rufen über den Button *Benutzer* den Benutzerzuordnungsdialog auf.

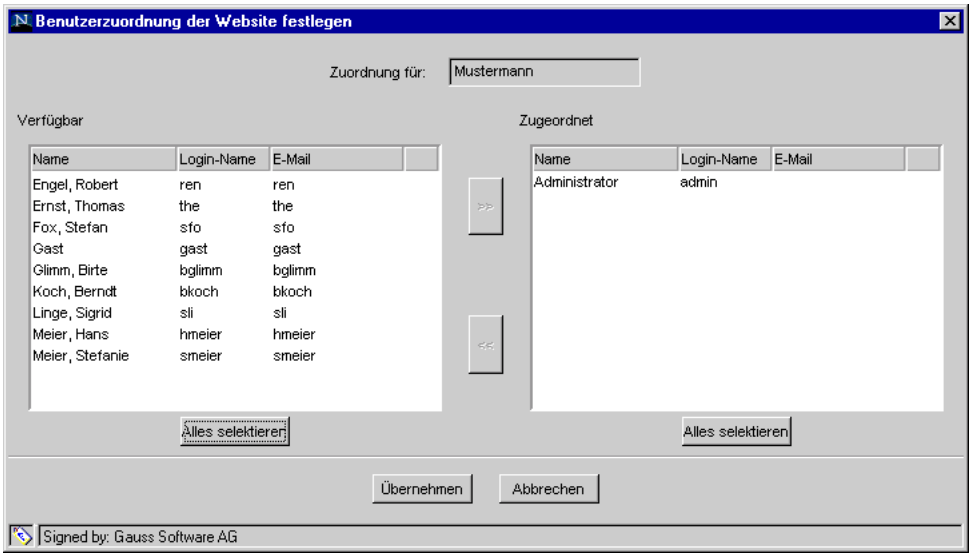

Abb. 28 – Dialog zur Zuordnung von Benutzern zu einer Website

Stellen Sie hier die gewünschte Benutzerzuordnung ein, und klicken Sie auf *Übernehmen*, um die Einstellung zu speichern.

5.3 Benutzer-Administration

Hinweis: Unmittelbar nach der Installation eines VIP-Systems ist nur der Benutzer “Administrator” in der Liste vorhanden.

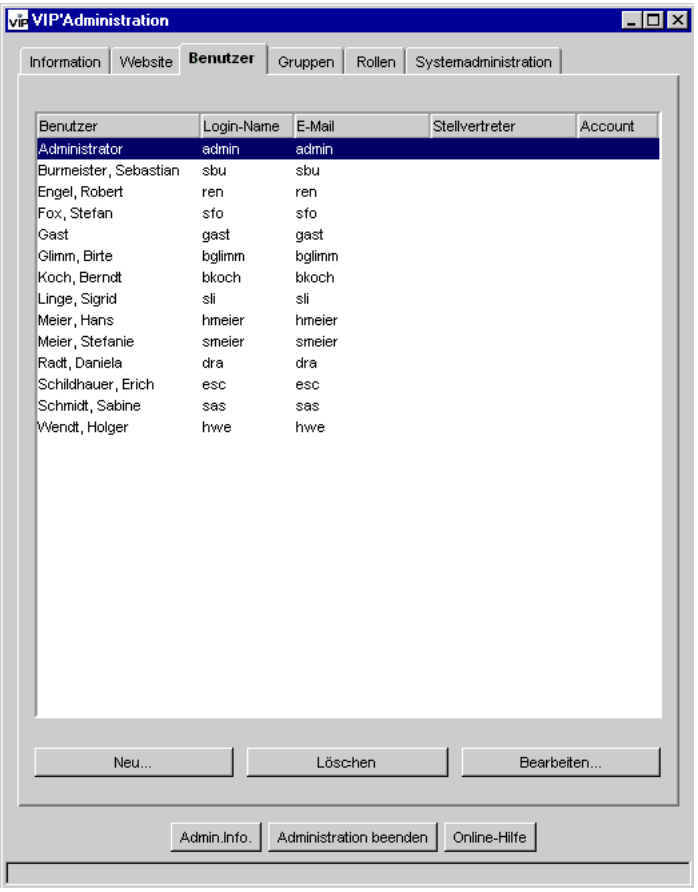

Abb. 29 – Dialog der Benutzer-Administration

Neuen Benutzer anlegen

Um einen neuen Benutzer anzulegen, klicken Sie in der Benutzer-Administration auf den Button *Neu*. Im darauffolgenden Dialog wird der neue Benutzer eingerichtet.

Abb. 30 – Dialog zum Anlegen eines neuen Benutzers

In die Felder des Dialogs werden folgende Informationen eingetragen:

Name: Der vollständige Benutzername, der den Benutzer innerhalb der VIP-Systeme identifiziert, z. B. *Meier Hans* oder *Meier, Dr. Hans* oder einfach *Hans*. Um eine übersichtliche Sortierung der Namen in der Benutzerverwaltung zu gewährleisten, sollte eine konsistente Schreibweise des Namens bei allen Benutzern verwendet werden. Für Benutzernamen dürfen folgende Zeichen verwendet werden:
a-z, A-Z, 0-9, Umlaute und “ß”, - (Bindestrich), _ (Unterstrich), . (Punkt) und (Leerzeichen)

Login-Name: Die Benutzerkennung, mit der sich der Benutzer in den VIP-Systemen anmelden soll, z. B. *hmeier* oder *HME* oder *hansm*. Beachten Sie bitte, daß Groß-

und Kleinbuchstaben bei der Benutzerkennung unterschieden werden. Der Benutzer mit dem Login-Namen *Hmeier* kann sich also nicht als *hmeier* oder *HMEIER* anmelden. Für Login-Namen dürfen nur folgende Zeichen verwendet werden:
a-z, A-Z, 0-9, - (Bindestrich), _ (Unterstrich) und . (Punkt)

E-Mail: Die Mailadresse des Benutzers. Für Mailadressen dürfen folgende Zeichen verwendet werden:
a-z, A-Z, 0-9, - (Bindestrich), _ (Unterstrich), . (Punkt) und @ (at-Zeichen)

Stellvertreter: Der für den Benutzer festgelegte Stellvertreter (nur Anzeige). Der Stellvertreter darf alle Funktionen ausführen, für die der Benutzer authorisiert ist.

Passwort: Das Paßwort, mit dem sich der Benutzer im VIP-System anmelden soll. Wie beim Login-Namen werden auch beim Paßwort Groß- und Kleinbuchstaben unterschieden. Für Paßwörter dürfen folgende Zeichen verwendet werden:
a-z, A-Z, 0-9, - (Bindestrich), _ (Unterstrich), . (Punkt) und @ (at-Zeichen)

Passwort bestätigen: Bestätigen Sie hier das Paßwort, um Fehleingaben zu vermeiden.

Sprache: Stellen Sie die bevorzugte Sprache des Benutzers ein. Die Benutzeroberflächen des VIP'ContentManager werden in der hier gewählten Sprache angezeigt. Durch eine Änderung dieser Einstellung für den Benutzer "admin" können Sie auch die Benutzeroberfläche des Administrationssystems auf eine andere Sprache einstellen.

Zugang sperren: Durch Aktivieren dieser Option kann das Account des Benutzers gesperrt werden, so daß er nicht mehr auf das VIP-System zugreifen kann.

Die Buttons im unteren Bereich des Dialogfensters rufen weitere Dialoge auf:

Gruppen: Klicken Sie hier, um den neuen Benutzer einer oder mehreren Gruppen zuzuordnen.

Rollen: Klicken Sie hier, um den neuen Benutzer einer oder mehreren Rollen zuzuordnen.

Rechte: Klicken Sie hier, um Standardvorgaben für die Zugriffsrechte des Benutzers festzulegen. Wenn der Benutzer zu den Zugriffsberechtigten eines Objekts hinzugefügt wird, erhält er zunächst die hier vorgegebenen Zugriffsrechte.

Stellvertreter: Klicken Sie hier, um einen Stellvertreter für den neuen Benutzer auszuwählen.

Funktionsbereiche: Klicken Sie hier, um den neuen Benutzer einem oder mehreren Funktionsbereichen zuzuordnen.

Klicken Sie auf *Speichern*, um die Angaben im System zu speichern und den Dialog zu schließen. Der neue Benutzer ist nun in der Benutzer-Administration eingetragen.

Benutzer ändern

Sie können die Benutzerdaten ändern, indem Sie in der Benutzer-Administration den gewünschten Benutzer auswählen und auf *Bearbeiten* klicken. Der Dialog zum Einrichten eines Benutzers erscheint (siehe Abbildung “Dialog zum Anlegen eines neuen Benutzers” auf Seite 134). Darin können Sie die gewünschten Änderungen vornehmen und durch einen Klick auf den Button *Speichern* im System speichern.

Benutzer löschen

Um einen Benutzer aus der Benutzerverwaltung Ihres VIP-Systems zu entfernen, wählen Sie in der Liste der Benutzer (im Dialog der Benutzerverwaltung) den entsprechenden Benutzer aus und klicken auf *Löschen*. Nachdem Sie den Vorgang bestätigt haben, wird der ausgewählte Benutzer aus der Liste entfernt. Dieser Benutzer kann sich dann nicht mehr im VIP-System anmelden.

> **Hinweis:** Ein Benutzer kann nicht gelöscht werden, wenn es in den Zugriffseinstellungen der Objekte im VIP-System *benutzerspezifische* Einstellungen für diesen Benutzer gibt. Dies wird vom Administrationssystem beim Löschvorgang automatisch geprüft. Wenn der Benutzer nicht gelöscht werden darf, erhalten Sie eine entsprechende Systemmeldung.

Vor dem Löschen eines solchen Benutzers müssen also alle benutzerspezifischen Zugriffseinstellungen des Benutzers gelöscht werden. Mit Hilfe des Objektfilters können Sie alle Objekte einer Website auffinden, bei denen es benutzerspezifische Zugriffseinstellungen für einen bestimmten Benutzer gibt.

Gruppenzuordnung festlegen

Im Dialog *Neuen Benutzer anlegen* bzw. *Benutzer bearbeiten* können Sie mit einem Klick auf den Button *Gruppen* den Gruppenzuordnungsdialog aufrufen.

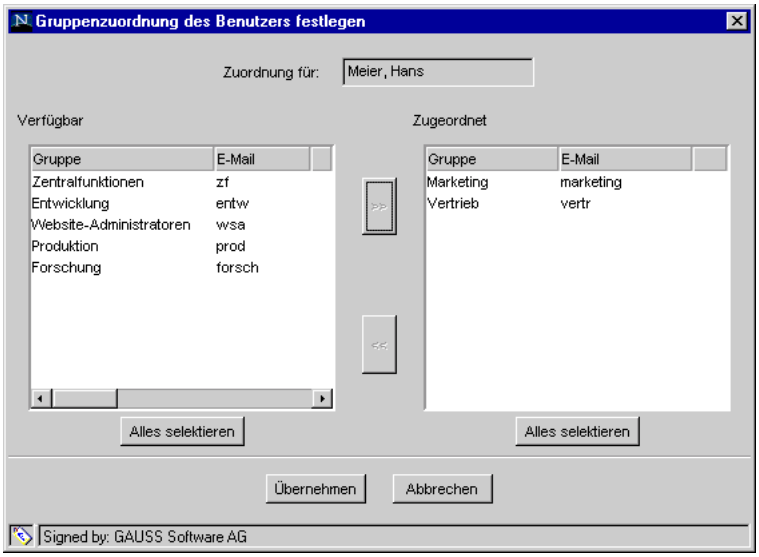

Abb. 31 – Dialog zum Zuordnen von Gruppen

In diesem Dialog legen Sie fest, welchen Gruppen der Benutzer zugeordnet wird. Klicken Sie auf *Übernehmen*, um die Einstellungen zu übernehmen und den Dialog zu schließen.

> **Hinweis:** Ihre Einstellungen werden erst im System gespeichert, wenn Sie im übergeordneten Dialog *Benutzer bearbeiten* bzw. *Neuen Benutzer anlegen* auf den Button *Speichern* klicken.

Rollenzuordnung festlegen

Im Dialog *Neuen Benutzer anlegen* bzw. *Benutzer bearbeiten* können Sie mit einem Klick auf den Button *Rollen* den Rollenzuordnungsdialog aufrufen. Hier können Sie die gewünschte Rollenzuordnung vornehmen.

Hinweis: Ihre Einstellungen werden erst im System gespeichert, wenn Sie im übergeordneten Dialog *Benutzer bearbeiten* bzw. *Neuen Benutzer anlegen* auf den Button *Speichern* klicken.

Stellvertreter zuordnen

Der Stellvertreter eines Benutzers kann jederzeit alle Funktionen ausüben, zu denen der Benutzer selbst berechtigt ist, vom Ausleihen eines Objekts bis zum Löschen eines kompletten Themas.

Der Stellvertreter eines Benutzers wird auf die gleiche Art und Weise festgelegt, wie die Gruppen- und Rollenzuordnung (siehe oben), wobei jedoch nur **ein** Stellvertreter pro Benutzer ausgewählt werden kann.

Klicken Sie im Dialog *Neuen Benutzer anlegen* bzw. *Benutzer bearbeiten* auf den Button *Stellvertreter*, um den entsprechenden Zuordnungsdialog *Stellvertreter festlegen* aufzurufen. Stellen Sie die gewünschte Zuordnung ein, und klicken Sie auf *Übernehmen*, um die Einstellung zu übernehmen und den Dialog zu schließen.

Hinweise:

Ihre Einstellungen werden erst im System gespeichert, wenn Sie im übergeordneten Dialog *Benutzer bearbeiten* bzw. *Neuen Benutzer anlegen* auf den Button *Speichern* klicken.

Für einen Benutzer kann es jeweils nur einen Stellvertreter geben. Wenn Sie für einen Benutzer bereits einen Stellvertreter festgelegt haben, müssen Sie diese Zuordnung zuerst zurücknehmen und dann den neuen Stellvertreter auswählen.

Standardzugriffsrechte einstellen

Im folgenden Dialog werden Standardvorgaben für die Zugriffsrechte eines Benutzers festgelegt. Die Zugriffsrechte sind Eigenschaften der einzelnen Objekte und können hier nicht geändert werden. Die Standardvorgaben werden lediglich als Vorschläge für die Zugriffsrechte angezeigt, sobald der Benutzer zur Liste der Zugriffsberechtigten eines Objekts hinzugefügt wird. Informationen zur Vergabe von Zugriffsrechten finden Sie in Kapitel 6 “Zugriffskontrolle”.

1. Klicken Sie im Dialog *Benutzer bearbeiten* (bzw. bereits beim Anlegen im Dialog *Neuen Benutzer anlegen*) auf den Button *Rechte*.

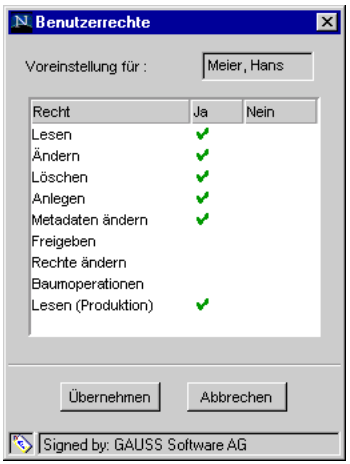

Abb. 32 – Dialog zur Voreinstellung der Benutzerrechte

2. Stellen Sie die gewünschten Standardvorgaben für die Zugriffsrechte des Benutzers ein, und klicken Sie dann auf *Übernehmen*, um die Einstellungen zu übernehmen und den Dialog zu schließen.

Hinweise:

Ihre Einstellungen werden erst im System gespeichert, wenn Sie im übergeordneten Dialog *Benutzer bearbeiten* bzw. *Neuen Benutzer anlegen* auf den Button *Speichern* klicken.

Wenn Sie – nachdem Sie den Benutzer einem Thema einer Website zugeordnet haben – die Benutzerrechte im Administrationssystem verändern, so haben diese Änderungen zunächst keine Auswirkungen. Damit die Rechteänderungen wirksam werden, müssen Sie den Benutzer im Pflegesystem zuerst aus dem entsprechenden Bereich der Website (z. B. aus einem Thema oder einem einzelnen VIP-Objekt) entfernen und ihn dann dem Bereich erneut zuweisen. Nehmen Sie diese Einstellungen im Dialog *Rechte* des Pflegesystems vor.

Funktionsbereiche einstellen

In den Funktionsbereichen sind im VIP'ContentManager spezielle Funktionen zusammengefaßt, die einem Benutzer nur zur Verfügung stehen, wenn er dem entsprechenden Funktionsbereich zugeordnet ist.

Durch Klicken auf den Button *Funktionsbereiche* im Dialog *Neuen Benutzer anlegen* bzw. *Benutzer bearbeiten* rufen Sie den Zuordnungsdialog für Funktionsbereiche auf. Stellen Sie in diesem Dialog die gewünschte Zuordnung für den Benutzer ein, und klicken Sie auf *Übernehmen*, um die Einstellung zu übernehmen und den Dialog zu schließen.

Hinweise:

Ihre Einstellungen werden erst im System gespeichert, wenn Sie im übergeordneten Dialog *Benutzer bearbeiten* bzw. *Neuen Benutzer anlegen* auf den Button *Speichern* klicken.

Wenn der Funktionsbereich eines Benutzers verändert wurde, muß der Benutzer sich erneut anmelden, damit die Änderungen wirksam werden.

Benutzerzugang sperren

Wenn Sie den Zugang eines Benutzers zu den VIP-Systemen verhindern möchten, können Sie dies durch folgende Änderung in der Benutzer-Administration erreichen:

1. Markieren Sie den Benutzereintrag in der Benutzer-Administration, und klicken Sie auf *Bearbeiten*.
2. Im Dialog *Benutzer bearbeiten* aktivieren Sie die Option *Zugang sperren*. Damit wird das Benutzer-Account gesperrt.
3. Klicken Sie dann auf *Speichern*, um diese Änderung im System zu speichern und den Dialog zu schließen.

5.4 Gruppen-Administration

Abb. 33 – Dialog zur Gruppen-Administration

Neue Gruppe anlegen

Um eine neue Gruppe anzulegen, klicken Sie in der Gruppen-Administration auf den Button *Neu*. Im darauffolgenden Dialog wird die neue Gruppe eingerichtet.

Abb. 34 – Dialog zum Anlegen einer neuen Gruppe

Gruppe: Geben Sie hier den Namen der Gruppe ein. Für Gruppennamen dürfen folgende Zeichen verwendet werden:
a-z, A-Z, 0-9, - (Bindestrich), _ (Unterstrich) und . (Punkt). Leerzeichen sind in Gruppennamen nicht zulässig.

E-Mail: Geben Sie hier die Mailadresse der Gruppe ein. Für Mailadressen dürfen folgende Zeichen verwendet werden:
a-z, A-Z, 0-9, - (Bindestrich), _ (Unterstrich), . (Punkt) und @ (at-Zeichen)

Rechte: Klicken Sie hier, um Standardvorgaben für die Zugriffsrechte der Gruppe einzustellen (siehe Abschnitt “Standardzugriffsrechte für Gruppen einstellen” auf Seite 146)).

Benutzer: Klicken Sie hier, um den Dialog für die Zuordnung von Benutzern aufzurufen (siehe Abschnitt “Zuordnung von Benutzern zu einer Gruppe” auf Seite 145).

Gruppe ändern

Sie können die Einstellungen einer Gruppe ändern, indem Sie in der Gruppen-Administration den entsprechenden Eintrag in der Liste der Gruppen auswählen und den Button *Bearbeiten* anklicken. Es erscheint der Dialog *Gruppe bearbeiten*. Darin können Sie die gewünschten Änderungen vornehmen und diese dann mit einem Klick auf den Button *Speichern* im System speichern.

Gruppe löschen

Um eine Gruppe zu löschen, wählen Sie in der Gruppen-Administration den entsprechenden Eintrag in der Liste der Gruppen aus und klicken auf den Button *Löschen*. Nach einer Sicherheitsabfrage wird die Gruppe aus der Liste entfernt und steht nicht mehr zur Verfügung.

> **Hinweis:** Beachten Sie bitte, daß es unter Umständen nicht möglich ist, eine Gruppe zu löschen, nämlich wenn es in den Zugriffseinstellungen der Objekte innerhalb des VIP-Systems spezifische Einstellungen für diese Gruppe gibt. Dies wird vom Administrationssystem beim Löschvorgang automatisch geprüft. Sie erhalten gegebenenfalls eine entsprechende Systemmeldung, wenn die Gruppe nicht gelöscht werden darf.

Vor dem Löschen einer Gruppe müssen also alle spezifischen Zugriffseinstellungen dieser Gruppe gelöscht werden. Mit Hilfe des Objektfilters können Sie alle Objekte einer Website auffinden, bei denen es solche Zugriffseinstellungen für eine bestimmte Gruppe gibt.

Zuordnung von Benutzern zu einer Gruppe

1. Wählen Sie in der Gruppen-Administration eine Gruppe aus, und klicken Sie auf den Button *Bearbeiten*. Es erscheint der Dialog *Gruppe bearbeiten*:

Abb. 35 – Dialog zum Bearbeiten einer Gruppe

2. Klicken Sie in diesem Dialog auf *Benutzer*. Damit wird der Benutzerzuordnungsdialog aufgerufen:

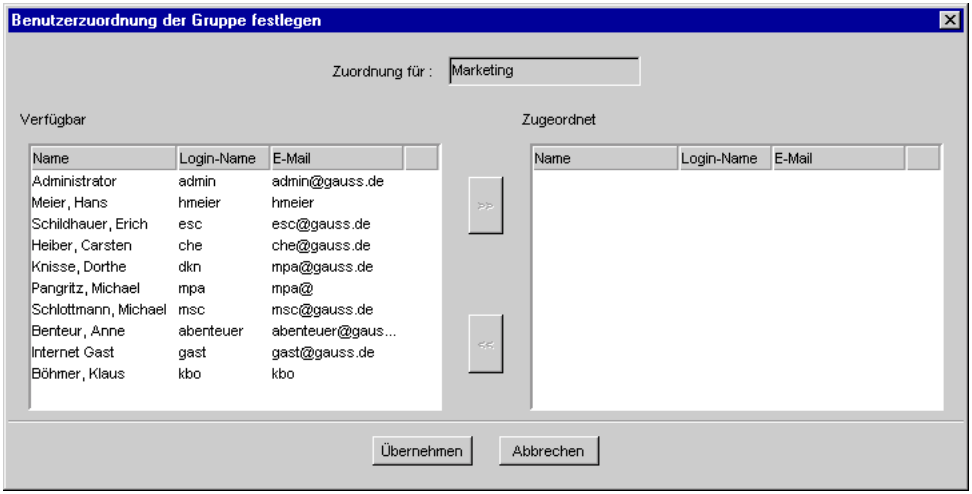

Abb. 36 – Dialog für die Zuordnung von Benutzern zu einer Gruppe

In diesem Dialog gibt es auf der einen Seite eine Liste aller verfügbaren Benutzer und auf der anderen Seite eine Liste der zugeordneten Benutzer.

3. Markieren Sie mit einem Mausklick die Benutzer, die der Gruppe zugeordnet werden sollen, und klicken Sie dann auf den Button, der zur Liste der zugeordneten Benutzer hinzeigt (Pfeil nach rechts). Die markierten Benutzer werden übernommen und erscheinen dann in der Zuordnungsliste (rechts).
4. Um einen Benutzer aus der Zuordnungsliste (rechts) wieder zu entfernen, markieren Sie mit einem Mausklick den entsprechenden Eintrag, und klicken Sie auf den Button, der von der Zuordnungsliste weg zeigt (Pfeil nach links).
5. Klicken Sie auf den Button *Übernehmen*, um diese Einstellungen zu übernehmen und den Zuordnungsdialog zu schließen.

Hinweis: Die Einstellungen werden erst im System gespeichert, wenn Sie im Dialog *Gruppe bearbeiten* auf den Button *Speichern* klicken.

Standardzugriffsrechte für Gruppen einstellen

Im folgenden Dialog werden Standardvorgaben für die Zugriffsrechte einer Gruppe festgelegt. Die Zugriffsrechte sind Eigenschaften der einzelnen Objekte und können hier nicht geändert werden. Die Standardvorgaben werden lediglich als Vorschläge für die Zugriffsrechte angezeigt, sobald die Gruppe zur Liste der Zugriffsberechtigten eines Objekts hinzugefügt wird. Informationen zur Vergabe von Zugriffsrechten finden Sie in Kapitel 6 “Zugriffskontrolle”.

1. Klicken Sie im Dialog *Gruppe bearbeiten* (bzw. bereits beim Anlegen im Dialog *Neue Gruppe anlegen*) auf den Button *Rechte*.

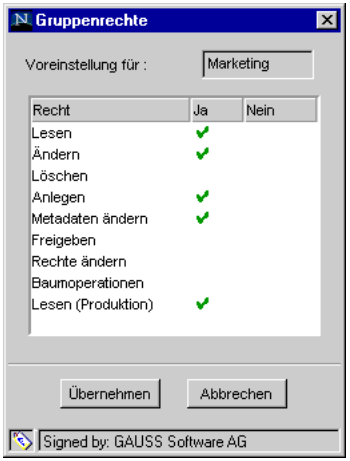

Abb. 37 – Dialog zur Voreinstellung der Zugriffsrechte

2. Stellen Sie die gewünschten Standardvorgaben für die Zugriffsrechte dieser Gruppe ein, und klicken Sie dann auf *Übernehmen*, um die Einstellungen zu übernehmen und den Dialog zu schließen.

Hinweise:

Ihre Einstellungen werden erst im System gespeichert, wenn Sie im übergeordneten Dialog *Gruppe bearbeiten* bzw. *Neue Gruppe anlegen* auf den Button *Speichern* klicken.

Wenn Sie – nachdem Sie die Gruppe einer Website zugeordnet haben – die Gruppenrechte im Administrationssystem verändern, so haben diese Änderungen zunächst keine Auswirkungen. Damit die Rechteänderungen wirksam werden, müssen Sie die Gruppe im Pflegesystem zuerst aus dem entsprechenden Bereich der Website (z. B. aus einem Thema oder einem einzelnen VIP-Objekt) entfernen und sie dann dem Bereich erneut zuweisen. Nehmen Sie diese Einstellungen im Dialog *Rechte* des Pflegesystems vor.

5.5 Rollen-Administration

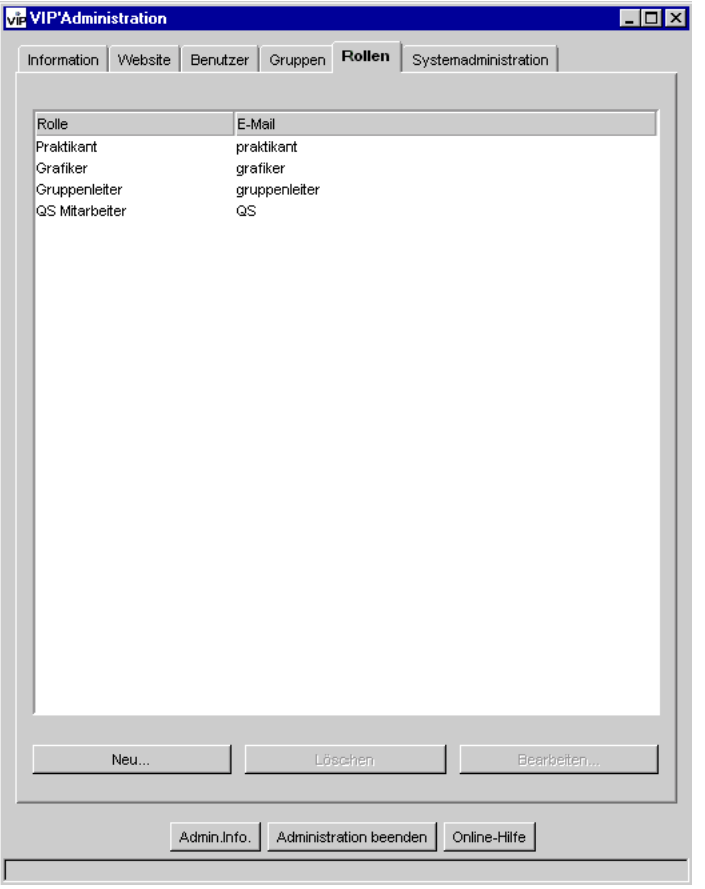

Abb. 38 – Dialog zur Rollen-Administration

Neue Rolle anlegen

Um eine neue Rolle anzulegen, klicken Sie in der Rollen-Administration auf den Button *Neu*. Im darauffolgenden Dialog wird die neue Rolle eingerichtet:

Abb. 39 – Dialog zum Einrichten einer neuen Rolle

Rolle: Geben Sie hier den Namen der Rolle ein. Für Rollennamen dürfen folgende Zeichen verwendet werden:
a-z, A-Z, 0-9, - (Bindestrich), _ (Unterstrich) und . (Punkt). Leerzeichen sind in Rollennamen nicht zulässig.

E-Mail: Geben Sie hier die Mailadresse der Rolle ein. Für Mailadressen dürfen folgende Zeichen verwendet werden:
a-z, A-Z, 0-9, - (Bindestrich), _ (Unterstrich), . (Punkt) und @ (at-Zeichen)

Rechte: Klicken Sie hier, um die Standardvorgaben für die Zugriffsrechte dieser Rolle einzustellen (siehe Abschnitt “Standardzugriffsrechte für Rollen einstellen” auf Seite 152).

Benutzer: Klicken Sie hier, um den Dialog zur Zuordnung von Benutzern aufzurufen (siehe “Zuordnung von Benutzern zu einer Rolle” auf Seite 150).

Rolle ändern

Sie können die Einstellungen einer Rolle ändern, indem Sie in der Rollen-Administration den entsprechenden Eintrag in der Liste der Rollen auswählen und den Button *Bearbeiten* anklicken. Es erscheint der Dialog *Rolle bearbeiten*. Darin

können Sie die gewünschten Änderungen vornehmen und diese dann mit einem Klick auf den Button *Speichern* im System sichern.

Rolle löschen

Um eine Rolle zu löschen, wählen Sie in der Rollen-Administration den entsprechenden Eintrag in der Liste der Rollen aus, und klicken Sie auf den Button *Löschen*. Nach einer Sicherheitsabfrage wird die Rolle aus der Liste entfernt und steht nicht mehr zur Verfügung.

Hinweis: Beachten Sie bitte, daß es unter Umständen nicht möglich ist, eine Rolle zu löschen, nämlich wenn diese exklusiven Zugriff auf Objekte innerhalb des VIP-Systems besitzt. Das Löschen der Rolle würde in diesem Fall dazu führen, daß der Zugriff auf diese Objekte nicht mehr möglich wäre. Vor dem Löschen empfiehlt es sich daher, die Zugriffsrechte der Rolle auf Objekte innerhalb des VIP-Systems zu prüfen und gegebenenfalls zu ändern.

Zuordnung von Benutzern zu einer Rolle

1. Wählen Sie in der Rollen-Administration eine Rolle aus, und klicken Sie auf den Button *Bearbeiten*. Es erscheint der Dialog *Rolle bearbeiten*.

Abb. 40 – Dialog zum Bearbeiten einer Rolle

2. In diesem Dialog klicken Sie auf *Benutzer*. Damit wird der Benutzerzuordnungsdialog aufgerufen:

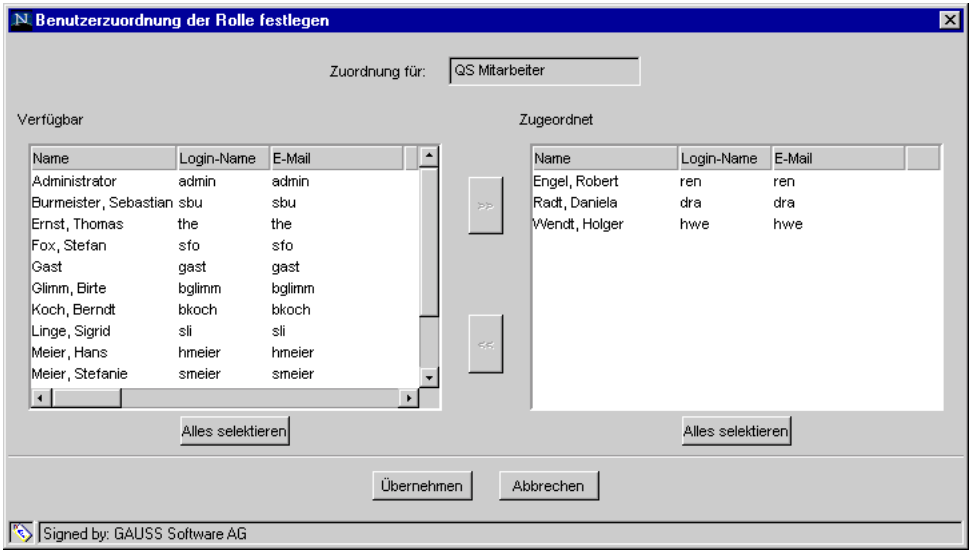

Abb. 41 – Dialog für die Zuordnung von Benutzern zu einer Rolle

3. Markieren Sie mit einem Mausklick die Benutzer, die der Rolle zugeordnet werden sollen, und klicken Sie dann auf den Button, der zur Liste der zugeordneten Benutzer hinzeigt (Pfeil nach rechts). Die markierten Benutzer werden übernommen und erscheinen dann in der Zuordnungsliste (rechts).
4. Um einen Benutzer aus der Zuordnungsliste (rechts) zu entfernen, markieren Sie mit einem Mausklick den entsprechenden Eintrag, und klicken Sie auf den Button, der von der Zuordnungsliste weg zeigt (Pfeil nach links).
5. Klicken Sie auf den Button *Übernehmen*, um diese Einstellungen zu übernehmen und den Zuordnungsdialog zu schließen.

Hinweis: Die Einstellungen werden erst im System gespeichert, wenn Sie im übergeordneten Dialog *Rolle bearbeiten* auf den Button *Speichern* klicken.

Standardzugriffsrechte für Rollen einstellen

Im folgenden Dialog werden Standardvorgaben für die Zugriffsrechte einer Rolle festgelegt. Die Zugriffsrechte sind Eigenschaften der einzelnen Objekte und können hier nicht geändert werden. Die Standardvorgaben werden lediglich als Vorschläge für die Zugriffsrechte angezeigt, sobald die Rolle zur Liste der Zugriffsberechtigten eines Objekts hinzugefügt wird. Informationen zur Vergabe von Zugriffsrechten finden Sie in Kapitel 6 “Zugriffskontrolle”.

1. Klicken Sie im Dialog *Rolle bearbeiten* (bzw. bereits beim Anlegen im Dialog *Neue Rolle anlegen*) auf den Button *Rechte*.

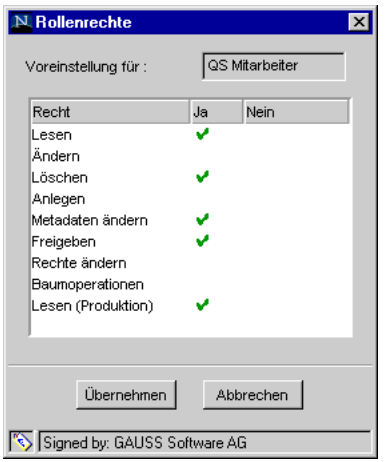

Abb. 42 – Dialog zur Voreinstellung der Zugriffsrechte

2. Stellen Sie die gewünschten Standardvorgaben für die Zugriffsrechte dieser Rolle ein, und klicken Sie dann auf *Übernehmen*, um die Einstellungen zu übernehmen und den Dialog zu schließen.

Hinweise:

Die Einstellungen werden erst im System gespeichert, wenn Sie im übergeordneten Dialog *Rolle bearbeiten* bzw. *Neue Rolle anlegen* auf den Button *Speichern* klicken.

Wenn Sie – nachdem Sie die Rolle einer Website zugeordnet haben – die Rollenrechte im Administrationssystem verändern, so haben diese Änderungen zunächst keine Auswirkungen. Damit die Rechteänderungen wirksam werden, müssen Sie die Rolle im Pflegesystem zuerst aus dem entsprechenden Bereich der Website (z. B. aus einem Thema oder einem einzelnen VIP-Objekt) entfernen und sie dann dem Bereich erneut zuweisen. Nehmen Sie diese Einstellungen im Dialog *Rechte* des Pflegesystems vor.

5.6 Systemadministration

Dieser Dialog dient zum stufenweisen Herunterfahren der VIP-Server. In der oberen Liste des Panels werden die aktiven Server angezeigt. In der unteren Liste werden die laufenden Prozesse dargestellt. Diese Liste kann entweder nach Aktionen (Abb. “Dialog zur Systemadministration”) oder Benutzern (Abb. “Aktionsliste nach Benutzern sortiert”) sortiert werden, indem Sie die entsprechende Option aktivieren.

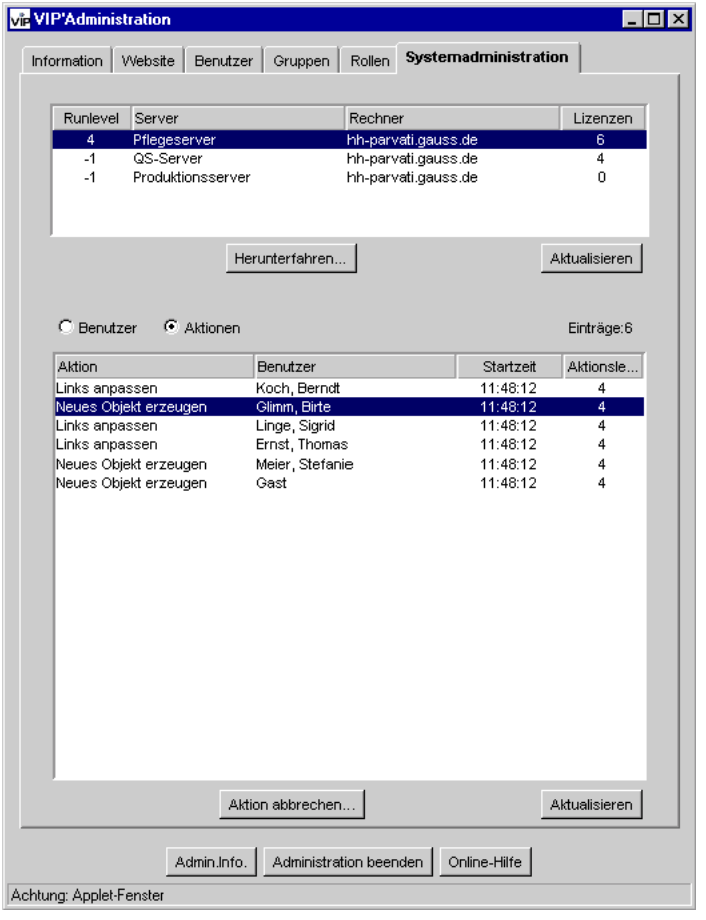

Abb. 43 – Dialog zur Systemadministration

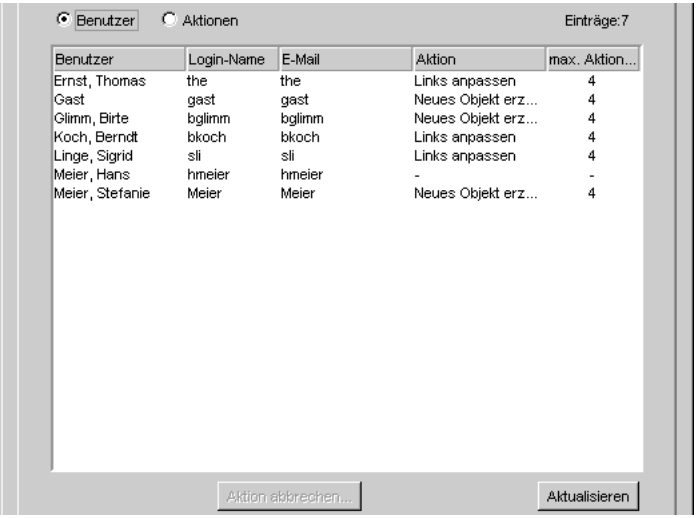

Abb. 44 – Aktionsliste nach Benutzern sortiert

Über den Button *Herunterfahren* rufen Sie den Dialog für das Beenden der Server auf. In diesem Dialog können Sie die zu beendenden Server auswählen und eine Nachricht für die Benutzer eingeben.

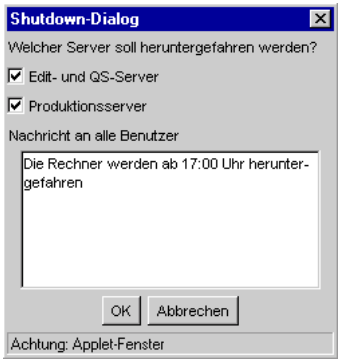

Abb. 45 – Dialog zum Beenden der Server

Das Herunterfahren der einzelnen Server geschieht stufenweise. Die auf den VIP-Servern ablaufenden Prozesse sind in sogenannte *Runlevel* von 0 bzw. -1 bis n eingeteilt. Der Runlevel ist ein Ordnungskriterium für die Ausführung bestimmter

Prozesse. Beim Herunterfahren der Server wird zuerst das Starten der Prozesse im höchsten Runlevel (n) abgelehnt, d. h. wenn ein Benutzer versucht, im VIP-System eine Aktion mit dem Runlevel n (z. B. direkte Freigabe eines Objekts) zu starten, wird die im Dialog zum Beenden der Server eingegebene Meldung angezeigt und die Aktion wird nicht ausgeführt.

Dadurch laufen alle Aktionen eines Runlevels nach und nach aus, da keine neuen Prozesse mehr gestartet werden. Wenn auf den herunterzufahrenden Servern in einem Runlevel alle Prozesse beendet sind, beginnt derselbe Vorgang für den nächsten Runlevel. Dies wird so lange wiederholt, bis sämtliche Prozesse auf den Servern beendet sind.

Langwierige Benutzeraktionen (oder bereits beendete, aber nicht ausgetragene Prozesse), die das Herunterfahren der Server unnötig verzögern, können aus der Liste gelöscht werden. Dazu markieren Sie den Eintrag für die abzubrechende Aktion und klicken auf den Button *Aktion abbrechen* oder wählen im Kontextmenü der rechten Maustaste die Option *Aktion abbrechen*. Bestätigen Sie den Vorgang im daraufhin angezeigten Dialog.

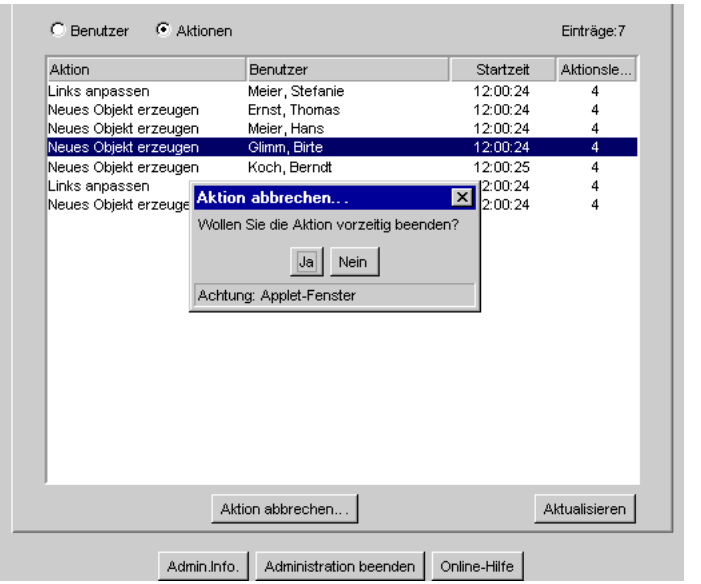

Abb. 46 – Dialog zum Abbrechen von langwierigen Aktionen

Hinweis: Klicken Sie regelmäßig auf den Button *Aktualisieren*, um die derzeit aktiven Serverprozesse anzeigen zu lassen.

Desweiteren weist der Dialog zur Systemadministration eine Spalte über die derzeit benutzten Lizenzen auf, wobei auch sämtliche Agenten sowie die VIP'XML ManagementConsole berücksichtigt werden.

Hinweis: Die Anzahl der derzeit benutzten Lizenzen kann von der Anzahl der angezeigten Benutzer abweichen. Genauere Informationen zu diesem Thema finden Sie auf der Support-Website SupPortal.

VIP-Server über Batch- bzw. Shell-Skript herunterfahren

Alternativ zum Herunterfahren der VIP-Server über den Admin-Client haben Sie die Möglichkeit, die Server über eine Skript-Datei zu beenden. Sie finden die Datei

- **startShutdownAgent.bat** bzw.
- **startShutdownAgent.sh**

im VIP-Installationsverzeichnis.

Hinweis: Bitte beachten Sie, daß Sie die **startShutdownAgent.bat** bzw. **startShutdownAgent.sh** aufrufen, die bei der Installation des VIP-Systems auf dem Server mitinstalliert wurde. Wenn Sie die entsprechende Datei nachträglich von der CD 1 "Versatile Installation Program" auf Ihr System kopieren, müssen Sie die Parameter `SERVER_NAME`, `SOCKET_PORT` und `HTTP_PORT` gemäß den Einstellungen auf Ihrem System anpassen. Darüber hinaus muß der JDK-Pfad unter `@SET PATH={JDK_PATH}` bzw. `JDKPATHNAME={JDK_PATH}` angegeben werden.

Wenn Sie die VIP-Server von einem anderen Rechner aus beenden möchten, als über den, auf dem sie installiert sind, muß zusätzlich folgendes beachtet werden:

1. Kopieren Sie die Datei **startShutdownAgent.bat** bzw. **startShutdownAgent.sh** auf den Rechner.

2. In dieser Kopie löschen Sie die Zeile `@cd admin` bzw. `cd admin`.
3. Geben Sie den JDK-Pfad unter `@SET PATH=` bzw. `JDKPATHNAME=` an.
4. Geben Sie unter `@SET mysys=` bzw. `mysys=` an, wo sich die Verzeichnisse mit den JAR-Dateien befinden, z. B. **v:\admin** oder **/remotevipshare/admin**. Wenn Sie auf das entsprechende Verzeichnis von Ihrem Rechner nicht zugreifen können, müssen Sie die JAR-Dateien **jndi.jar**, **ldap.jar, providerutil.jar** und **vipadmin.jar** kopieren und in den oben beschriebenen Parametern das entsprechende Verzeichnis eintragen. Die Dateien sind wie folgt anzugeben (unterhalb des in `mysys=` angegebenen Verzeichnisses):

Tabelle 4 – Dateiangabe unter Windows NT und Unix

Windows NT	Unix
lib\jndi.jar	**lib/jndi.jar**
lib\ldap.jar	**lib/ldap.jar**
lib\providerutil.jar	**lib/providerutil.jar**
java\vipadmin.jar	**java/vipadmin.jar**

Der Aufruf des Skripts bewirkt folgendes:

- Die Aktionen der jeweiligen Runlevel laufen nach und nach aus.
- Das Event `SERVER_DOWN` wird ausgelöst.
- Die Methode `stop()` wird bei allen Agenten aufgerufen.
- Das VIP-System wird beendet.

Im Extremfall, d. h. wenn die VIP-Server nicht wie oben beschrieben heruntergefahren werden können, besteht die Möglichkeit, sie mit der Option `-emergency` herunterzufahren.

Achtung: Diese Option darf **nicht** standardmäßig zum Herunterfahren der VIP-Server angewandt werden.

Fahren Sie die VIP-Server nur mit der Option `-emergency` herunter, wenn folgende Umstände gegeben sind:

- Das Herunterfahren der Server konnte auch nach einem längeren Zeitraum nicht durchgeführt werden.
- Die Angabe der Runlevel der herunterzufahrenden Server im Administrationssystem ändert sich nicht mehr.
- Es laufen keine aufwendigen Operationen, wie z. B. komplexe Baumoperationen.
- In der entsprechenden Website finden keine Veränderungen statt, wie z. B. das Anlegen neuer Dateien.

Rufen Sie das Skript wie folgt auf:

```
StartShutDownAgent -emergency
```

Der Aufruf des Skripts bewirkt in diesem Fall folgendes:

- Das Event `SERVER_DOWN` wird sofort ausgelöst.
- Die Methode `stop()` wird bei allen Agenten aufgerufen.
- Das VIP-System wird beendet.

5.7 Datenabgleich mit dem LDAP-Server

Die Konfiguration einer LDAP-Anbindung wird im Abschnitt 4.5 “Konfiguration einer LDAP-Anbindung” auf Seite 76 beschrieben. Nachdem Sie die Verbindung zum Verzeichnisdienst hergestellt haben, können Sie Daten aus dem Verzeichnisdienst in das VIP-Administrationssystem übernehmen.

Abgleich mit dem Verzeichnisdienst durchführen

Um das VIP-Administrationssystem mit dem Verzeichnisdienst abzugleichen und dadurch die Daten des Verzeichnisdienstes – wie in der Konfiguration festgelegt – ins VIP-Administrationssystem zu übernehmen, gehen Sie folgendermaßen vor:

1. Vergewissern Sie sich, daß der LDAP-Server läuft und die Konfiguration korrekt ist.
2. Öffnen Sie im VIP-Administrationssystem das Panel *LDAP*.

   Hinweis: Das LDAP-Panel ist nur verfügbar, wenn in der Konfigurationsdatei **directory.properties** der Eintrag LDAP=ON gesetzt ist.

   Sie können den Abgleich mit dem LDAP-Server auch über die Eingabe einer Kommandozeile veranlassen. Weitere Informationen dazu finden Sie im Abschnitt “LDAP Batch-Abgleich” auf Seite 87.

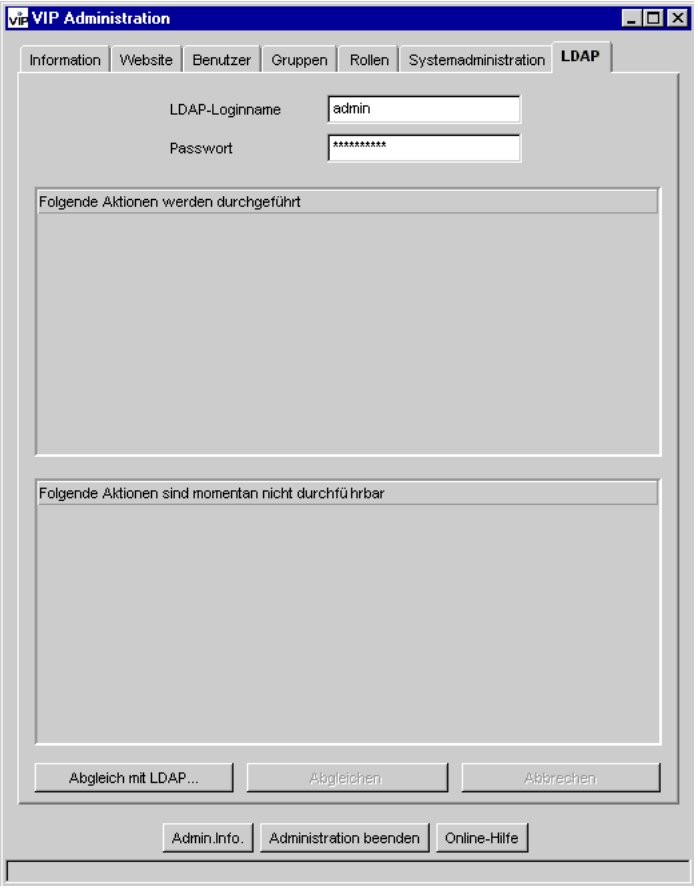

Abb. 47 – LDAP-Panel des VIP-Administrationssystems

3. Klicken Sie auf den Button *Abgleich mit LDAP*. Die bestehenden Daten des VIP-Administrationssystems werden mit dem aktuellen Datenbestand des Verzeichnisdienstes verglichen. Nach Abschluß dieses Vergleichs werden die Ergebnisse angezeigt.

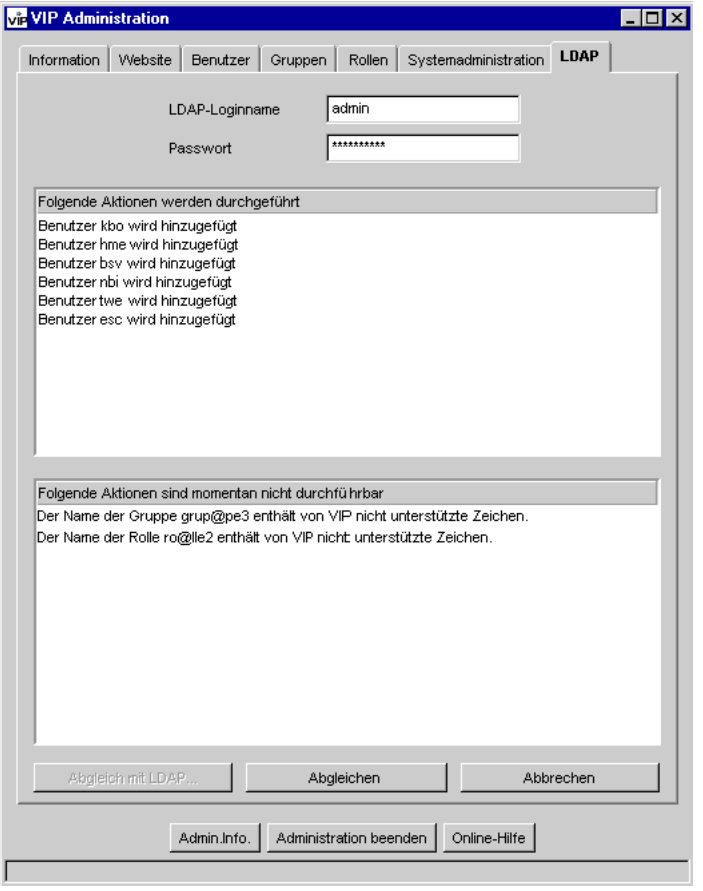

Abb. 48 – Ergebnis der Abgleichprüfung mit LDAP

4. Klicken Sie auf den Button *Abgleichen*, um die Daten wie angezeigt zu übernehmen.

5.8 Funktionsbereiche

Die Funktionsbereiche bieten spezielle Funktionen, die nur von ausgewählten Benutzern durchgeführt werden können. Die Erlaubnis, in einem solchen Funktionsbereich zu arbeiten, wird in der Benutzer-Administration festgelegt.

Um einem Benutzer die Arbeit in einem Funktionsbereich zu ermöglichen, wählen Sie den entsprechenden Benutzer in der Benutzer-Administration aus, und klicken Sie auf den Button *Bearbeiten*. Im Dialog *Benutzer bearbeiten* klicken Sie auf *Funktionsbereiche*. Damit wird der Zuordnungsdialog aufgerufen, in dem Sie die Funktionsbereiche des Benutzers einstellen können.

Objekte anlegen

Über die Funktionsbereiche wird festgelegt, welche Objekte von dem jeweiligen Benutzer angelegt werden dürfen. So dürfen Benutzer, die einem bestimmten Funktionsbereich (z. B. VIP) zugeordnet wurden, nur gewisse Objekttypen anlegen. In der folgenden Tabelle wird dargestellt, welche Funktionsbereiche Sie dem Benutzer zuordnen müssen, damit er das entsprechende Objekt anlegen darf.

Tabelle 5 – Funktionsbereiche und Objekte

Zugeordneter Funktionsbereich	Anzulegender Objekttyp
VIP	HTML, Thema, Sonstige, Grafik, Verbund, PDF, MS Excel, MS Word, MS PowerPoint
Erweiterte Funktionen	Vorlage, Frame, Frame-Thema, CGI Skript
Dynamische Typen	ASP, ASP-Thema, PHP, PHP-Thema, STM, STM-Thema, JSP, JSP-Thema
ITF	JSP-Vorlage, Formularvorlage
Formular Instanz	Formularinstanz

Hinweis: Bitte beachten Sie, daß keine Formularinstanzen über die Client-Oberfläche angelegt werden sollten.

In den folgenden Abschnitten wird beschrieben, welche Funktionen die Benutzer ausführen dürfen, die den Funktionsbereichen “Direkte Freigabe”, “HTML-Tag einfügen”, “VIP-Objekt einfügen” und “VIP_DBC_ADMIN” zugeordnet sind.

Objekte mit der Option *direkte Freigabe* anlegen

Mit der Option *direkte Freigabe* kann der Workflow eines Objekts gegenüber dem Standardworkflow von VIP-Objekten geändert werden. Wenn ein Objekt mit der Option *direkte Freigabe* angelegt wird, kann das Objekt direkt aus dem Pflegesystem freigegeben werden. Die erste Freigabe des Objekts muß jedoch (dem Standardworkflow entsprechend) durch die Qualitätssicherung erfolgen.

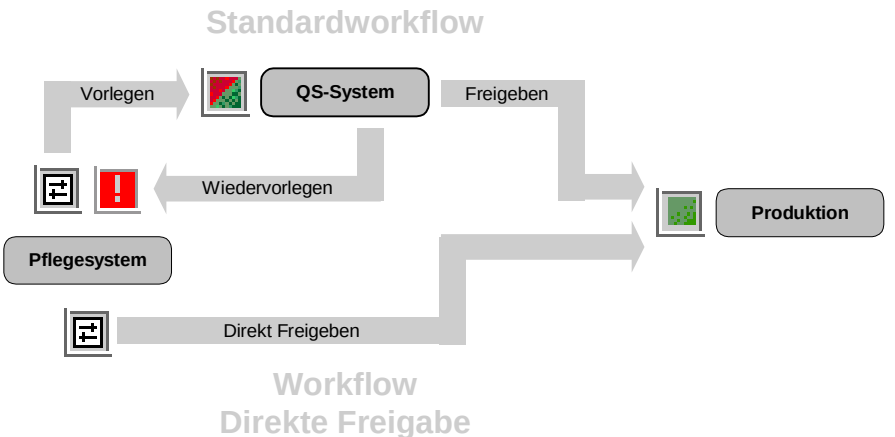

Abb. 49 – Workflow bei direkter Freigabe

Nach der ersten Freigabe durch die Qualitätssicherung können an einem solchen Objekt beliebige Änderungen vorgenommen und direkt aus dem Pflegesystem freigegeben werden. Die Seiten unterliegen dann nicht mehr der Kontrolle der Qualitätssicherung.

Für die verschiedenen Funktionen im Zusammenhang mit der direkten Freigabe sind die folgenden Zugriffsrechte bzw. Funktionsbereiche erforderlich:

- **Anlegen mit direkter Freigabe –** Um ein Objekt mit der Option *direkte Freigabe* anzulegen, muß der Benutzer über das Anlegerecht unterhalb des entsprechenden Themas verfügen und dem Funktionsbereich “direkte Freigabe” zugeordnet sein.
- **Erste Freigabe** – Die erste Freigabe muß durch die Qualitätssicherung vorgenommen werden (Standardworkflow). Um das Objekt in der Qualitätssicherung freizugeben, braucht der Benutzer das Freigaberecht.
- **Änderungen direkt freigeben –** Um das Objekt nach der ersten Freigabe direkt aus dem Pflegesystem freizugeben, braucht der Benutzer nur das Recht zum Bearbeiten.

Zur Verdeutlichung hier ein Beispiel:

Herr Koch möchte den Speiseplan der Kantine in das Intranet einpflegen und ist der Meinung, daß diese Informationen nicht jede Woche von der Qualitätssicherung geprüft werden müssen. Er möchte also, daß der Speiseplan mit der Option *direkte Freigabe* angelegt wird. Herr Koch hat unter dem Thema “Betriebsinformationen” zwar das Anlegerecht, er ist aber nicht dem Funktionsbereich “Anlegen mit direkter Freigabe” zugeordnet. Den Speiseplan kann Herr Koch also nicht selbst mit der Option *direkte Freigabe* anlegen. Er bittet also seinen Gruppenleiter, Herrn Haupt, das Objekt für ihn anzulegen:

Herr Haupt verfügt ebenfalls über das Recht, unter dem Thema “Betriebsinformationen” Objekte anzulegen und zu ändern. Darüber hinaus ist er dem Funktionsbereich “Anlegen mit direkter Freigabe” zugeordnet. Er kann also den Speiseplan unter dem Thema “Betriebsinformationen” für Herrn Koch mit der Option *direkte Freigabe* anlegen. Da Herr Haupt auch über das Recht verfügt, unter dem Thema “Betriebsinformationen” die Zugriffsrechte zu ändern, kann er Herrn Koch das Recht verleihen, das neue Objekt zu bearbeiten.

Nun fügt Herr Koch den aktuellen Speiseplan in dieses Objekt ein. Das Objekt kann er aber noch nicht direkt freigeben. Die erste Freigabe muß durch die Qualitätssicherung erfolgen. Herr Koch legt den Speiseplan also zur Qualitätssicherung vor.

In der Qualitätssicherung wird der Speiseplan von Frau Tieken geprüft. Sie findet ihn ausgesprochen lecker und gibt ihn frei. Danach steht der Speiseplan im Intranet und kann jederzeit von Herrn Koch bearbeitet und direkt freigegeben werden.

Objekte mit der Option *HTML-Tag einfügen* anlegen

Mit der Option *HTML-Tag einfügen* kann beim Anlegen eines neuen Objekts ein HTML-Tag definiert werden, der in das neue Objekt integriert wird. Um ein Objekt mit der Option *HTML-Tag einfügen* anlegen zu können, sind folgende Voraussetzungen notwendig:

- Der Benutzer muß über das Anlegerecht unterhalb des entsprechenden Themas verfügen.
- Der Benutzer muß dem Funktionsbereich “HTML-Tag einfügen” zugeordnet sein.

Objekte mit der Option *VIP-Objekt einfügen* anlegen

Mit der Option *VIP-Objekt einfügen* kann beim Anlegen eines neuen Objekts ein VIP-Objekt festgelegt werden, das in das neue Objekt integriert wird. Um ein Objekt mit der Option *VIP-Objekt einfügen* anlegen zu können, sind folgende Voraussetzungen notwendig:

- Der Benutzer muß über das Anlegerecht unterhalb des entsprechenden Themas verfügen.
- Der Benutzer muß dem Funktionsbereich “VIP-Objekt einfügen” zugeordnet sein.

Tabellen mit dem VIP’DBC Editor anlegen und bearbeiten

Mit dem VIP’DBC-Editor können CSV-, ISAM- und JDBC-Tabellen angelegt und bearbeitet werden. Dazu muß folgende Voraussetzung erfüllt sein:

- Der Benutzer muß dem Funktionsbereich “VIP_DBC_ADMIN” zugeordnet sein.

Weitere Informationen zum Anlegen und Bearbeiten von Tabellen mit dem VIP’DBC Editor finden Sie im Kapitel 7 “Arbeiten mit dem VIP’DBC Editor”.

KAPITEL 6

Zugriffskontrolle

Durch die Funktionen der Zugriffskontrolle kann im VIP'ContentManager der Zugriff auf die Objekte einer Website genau bestimmt werden. Die Benutzer der Website erhalten – aufgrund von objektspezifischen Zugriffseinstellungen – das Recht, auf Objekte zuzugreifen, und zwar mit bestimmten Zugriffsrechten. Über die Zugriffseinstellungen wird festgelegt, wie die Benutzer auf die Objekte der Website zugreifen können, z. B. ob sie die Objekte nur lesen oder auch ändern dürfen.

Die Möglichkeiten der Zugriffskontrolle sind nicht nur umfangreich, sondern auch variabel einsetzbar. Sie ermöglichen den Aufbau von sehr unterschiedlichen Zugriffskontrollsystemen, von einer einfachen Gruppenverwaltung bis hin zu komplexen Kontrollsystemen für sicherheitsrelevante Bereiche. Die Zugriffskontrolle kann also exakt auf die Anforderungen Ihrer Organisation abgestimmt werden. Wenn Sie mit einem klaren Zugriffskonzept beginnen, können Sie im VIP'ContentManager ohne großen Aufwand den Objektzugriff regeln und auf die Aufgaben und Erfordernisse der verschiedenen Benutzer abstimmen.

Für die Verwaltung der Zugriffsrechte sind unter anderem folgende Themen von grundlegender Bedeutung:

- objektspezifische Zugriffsrechte
- Prinzip der Vererbung
- Standardmäßige Zugriffsrechte
- Vorrangsregelung
- aufgabenbezogene Zugriffsrechte
- Benutzer-, Gruppen- und Rollen-Administration

6.1 Objektspezifische Zugriffsrechte

Welche Benutzer, Gruppen oder Rollen auf ein Objekt zugreifen dürfen, ist in den Eigenschaften des Objekts festgelegt. Die Zugriffsrechte können für jedes Objekt spezifisch eingestellt werden. Dadurch ist es nicht nur möglich, den Zugriff generell zu erlauben oder zu verbieten, sondern es können für die einzelnen Benutzer, Gruppen und Rollen jeweils spezifische Zugriffsmodi eingestellt werden.

Jedes der folgenden Zugriffsrechte kann in den Einstellungen eines Objekts einem Benutzer (bzw. einer Gruppe oder Rolle) explizit verliehen oder verwehrt werden:

Lesen	Der Benutzer darf das Objekt lesen.
Bearbeiten	Der Benutzer darf das Objekt im Pflegesystem ausleihen, ändern, zurückgeben und der Qualitätssicherung vorlegen. Bei Objekten, die mit der Option *direkte Freigabe* angelegt wurden, kann der Benutzer diese auch freigeben.
Anlegen	Der Benutzer darf unterhalb dieses Themas neue Objekte anlegen.
Löschen	Der Benutzer darf das Objekt löschen. Dies ist aber nur im Qualitätssicherungssystem unter den einschlägigen Bedingungen möglich.
Freigeben	Der Benutzer darf diese Seite im Qualitätssicherungssystem freigeben und dadurch im Produktionssystem veröffentlichen.
Metadaten ändern	Der Benutzer darf die Metadaten des Objekts ändern. Damit können verschiedene Eigenschaften des Objekts geändert werden, z. B. das Ablaufdatum, der Titel oder die Vorlage.
Zugriffsrechte ändern	Der Benutzer darf die Zugriffsrechte auf dieses Objekt ändern.

Baumoperationen	Der Benutzer darf dieses Objekt kopieren und (in Verbindung mit dem Anlegerecht) an einer anderen Stelle in der Objekthierarchie einfügen. Um das Objekt von seiner ursprünglichen Stelle zu verschieben, braucht der Benutzer zusätzlich das Änderungsrecht.
Lesen (Produktion)	Der Benutzer darf dieses Objekt im Produktionssystem lesen (siehe “Zugriffsrechte für das Produktionssystem einstellen” auf Seite 182).

6.2 Vererbung von Zugriffsrechten

Die Zugriffseinstellungen eines Themas werden automatisch an die darunter angelegten Seiten, Themen und andere Objekte weitergegeben. Das bedeutet, Sie können für Ihre Hauptthemen die Zugriffsrechte einmal einstellen und müssen sich nicht um die untergeordneten Objekte kümmern. Diese Weitergabe der eingestellten Zugriffsrechte an untergeordnete Objekte wird *Vererbung* genannt. Die Zugriffseinstellungen eines Themas werden also an die darunter angelegten Objekte vererbt.

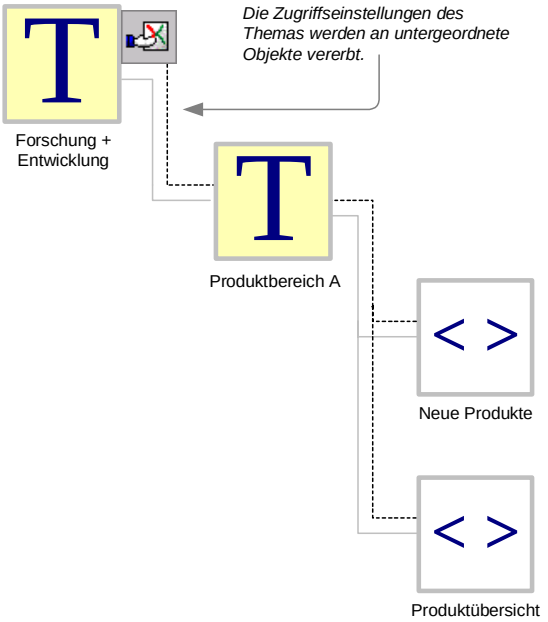

Abb. 50 – Vererbung von Zugriffsrechten

Aufgrund der Vererbung von Zugriffseinstellungen an untergeordnete Objekte können die Zugriffsrechte für eine Website mit wenig Aufwand so eingestellt werden, daß verschiedene Benutzergruppen mit unterschiedlichen Aufgabenbereichen entsprechend auf die Themen und Objekte der Website zugreifen können. Jedes neu angelegte Objekt erbt die Zugriffsrechte des Themas, zu dem es gehört. Wenn Sie also bestimmten Gruppen, Rollen oder Benutzern den Zugriff auf ein Thema eingeräumt haben, bekommen diese automatisch die gleichen Zugriffsrechte auf neue Seiten oder Themen, die unterhalb des Themas angelegt werden.

Die vom Thema geerbten Zugriffsrechte können jederzeit geändert werden. Eine solche Änderung der Zugriffsrechte kann jedoch nur von Benutzern vorgenommen werden, die über das Änderungsrecht für die Zugriffsrechte verfügen. Die geänderten Einstellungen werden ihrerseits nach unten – an die darunter angelegten Objekte – vererbt.

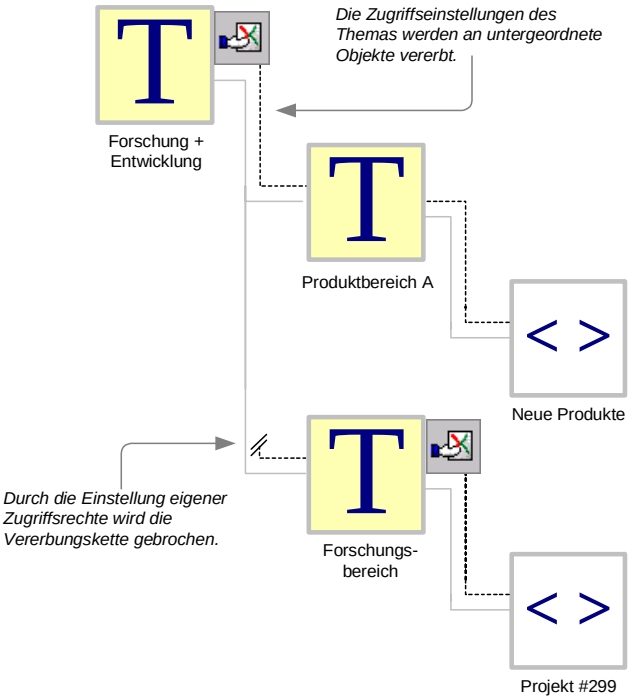
Die Zugriffseinstellungen des Themas werden an untergeordnete Objekte vererbt.
Forschung + Entwicklung
Produktbereich A
Neue Produkte
Durch die Einstellung eigener Zugriffsrechte wird die Vererbungskette gebrochen.
Forschungs-bereich
Projekt #299

Abb. 51 – Geänderte Zugriffsrechte

Jede Änderung der Zugriffsrechte eines Objekts unterbricht die Vererbung vom übergeordneten Thema. Handelt es sich bei dem Objekt um ein Thema, entsteht an dieser Stelle eine neue Vererbungskette. Die unter diesem Thema angelegten Objekte erhalten die neuen, geänderten Zugriffseinstellungen.

Wenn Sie nachträglich die Zugriffsrechte eines Thema ändern, betrifft diese Änderung nicht nur das Thema selbst, sondern auch alle Objekte in der Vererbungskette des Themas. Auf die Objekte in einer anderen Vererbungskette hat die Änderung dagegen keinen Einfluß.

Um die geänderten Zugriffsrechte eines Objekts aufzuheben und das Objekt wieder in die Vererbungskette des übergeordneten Themas einzugliedern, rufen Sie die Zugriffseinstellungen des Objekts auf und klicken auf den Button *Standard-ACL*.

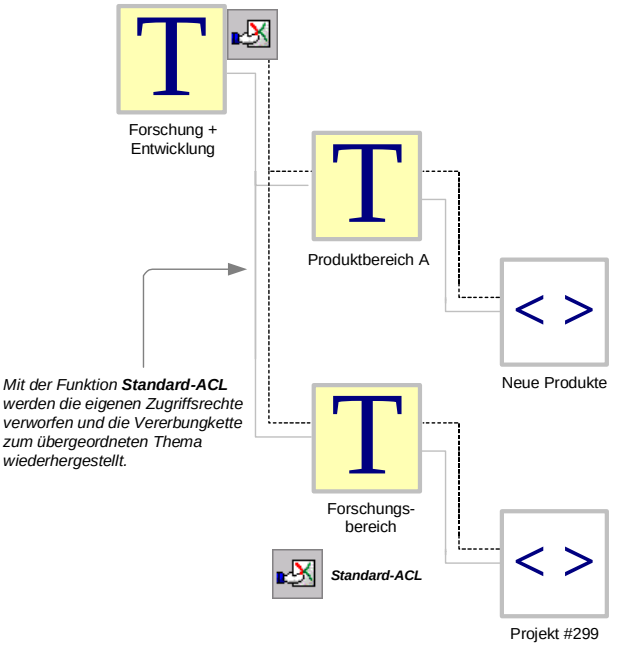

Abb. 52 – Wiederherstellen der vererbten Zugriffsrechte

Damit werden die geänderten Zugriffsrechte des Objekts verworfen und die Vererbung vom übergeordneten Thema wiederhergestellt.

6.3 Standardmäßige Zugriffsrechte

Grundsätzlich gilt, daß ein Benutzer erst dann auf ein Objekt zugreifen kann, wenn er über das entsprechende Zugriffsrecht verfügt. Das bedeutet, daß es in der Regel nicht erforderlich ist, einen bestimmten Zugriff explizit zu verbieten. Solange er nicht ausdrücklich erlaubt oder von einem übergeordneten Thema vererbt wird, ist der Zugriff standardmäßig verboten.

Wenn Sie die Arbeit in einem bestimmten Themenbereich nur einer bestimmten Benutzergruppe erlauben möchten, ist es nicht erforderlich, für alle anderen Gruppen ein Zugriffsverbot auf die Objekte in diesem Bereich zu verhängen. Sie

räumen einfach der einen Gruppe das entsprechende Zugriffsrecht ein. Für alle anderen gilt: Was nicht explizit erlaubt wurde, ist verboten.

6.4 Vorrangsregeln

Das Zugriffsrecht eines Benutzers auf ein Objekt kann aus seiner Zugehörigkeit zu einer Gruppe bzw. Rolle oder den benutzerspezifischen Einstellungen hervorgehen. Das Zugriffsrecht ergibt sich aus der Kombination von gruppen- und rollenspezifischen Rechten mit den benutzerspezifischen Rechten.

Da die Zugriffsrechte auf ein Objekt für Gruppen, Rollen und einzelne Benutzer verschieden definiert sein können, ist es möglich, daß die Zugriffsrechte eines Benutzers aufgrund seiner Gruppenzugehörigkeit, seiner Rollenzuordnung und seiner individuellen Zugriffsrechte widersprüchlich sind. Solche Widersprüche werden anhand der folgenden Vorrangsregeln aufgelöst:

1. Ein explizites Verbot hat zunächst Vorrang vor einer expliziten Erlaubnis.
2. Eine individuelle explizite Erlaubnis hebt ein allgemeines bzw. gruppen- oder rollenspezifisches Verbot auf.
3. Ist der Zugriff weder explizit verboten noch erlaubt, gilt ein implizites Verbot (das heißt, der Zugriff ist nicht möglich).

Diese Vorrangsregeln sollen an einem einfachen Beispiel verdeutlicht werden:

Der Benutzer “HaraldW” ist Praktikant im Bereich “Zentralfunktionen”. Er bekommt die Aufgabe, verschiedene Seiten des Intranets zu pflegen, unter anderem die Telefonliste und den Raumbelegungsplan für Konferenzräume.

Im Administrationssystem wird “HaraldW” der Gruppe “Zentralfunktionen” und der Rolle “Praktikant” zugeordnet. Dadurch erhält er Zugriffsrechte auf die Objekte unter dem Thema “Betriebsinformationen”. Die Zugriffsrechte sind aufgrund seiner Gruppen- und Rollenzuordnung folgendermaßen eingestellt:

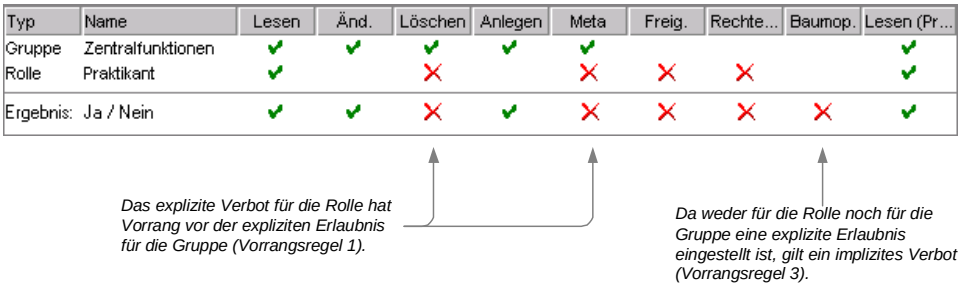

Abb. 53 – Zugriffsrechte aufgrund der Gruppen- und Rollenzuordnung

Die verschiedenen Seiten unter “Betriebsinformationen” sollen von “HaraldW” regelmäßig aktualisiert werden. Dabei soll der Praktikant auch darauf achten, daß für jede Seite ein angemessenes Ablaufdatum eingestellt ist. Gegebenenfalls soll er das Ablaufdatum in den Metadaten neu einstellen.

Die Zugriffsrechte für die Rolle “Praktikant” sind so eingestellt, daß Änderungen an den Metadaten nicht erlaubt sind. Dieses explizite Verbot, die Metadaten zu ändern, hat auch Vorrang vor der Erlaubnis für die Gruppe “Zentralfunktionen”. Das Ergebnis dieser Einstellungen ist also, daß “HaraldW” die Metadaten der Seiten nicht ändern kann.

Es gibt mehrere Möglichkeiten, dem Benutzer “HaraldW” die erforderlichen Zugriffsrechte zum Ändern von Metadaten zu geben:

- Der Benutzer “HaraldW” wird aus der Rolle “Praktikant” herausgenommen. Damit werden seine Zugriffsrechte auf diese Objekte allein durch die Zuordnung zur Gruppe “Zentralfunktionen” bestimmt. Durch die Gruppenzuordnung (ohne die rollenspezifischen Einschränkungen) hätte er aber nicht nur das Recht zum Ändern von Metadaten, sondern auch zum Löschen von Objekten.
- Die Zugriffseinstellungen für die Rolle “Praktikant” werden geändert, so daß das Ändern von Metadaten nicht explizit verboten ist. Dies würde aber für alle Praktikanten gelten, nicht nur für “HaraldW”.
- Für den Benutzer “HaraldW” wird eine explizite Erlaubnis zum Ändern von Metadaten eingestellt. Das Verbot aufgrund der Rollenzuordnung wird nämlich durch eine solche benutzerspezifische Erlaubnis wieder aufgehoben.

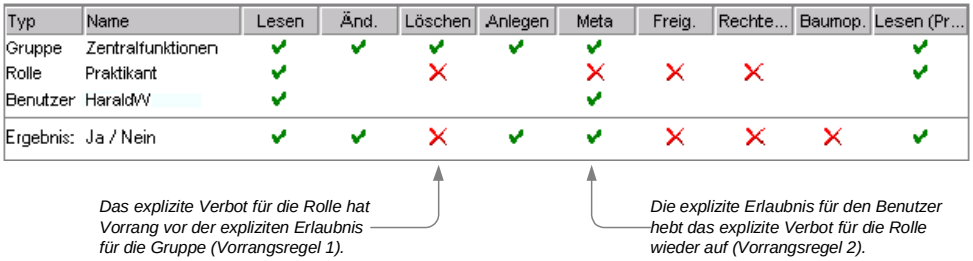

Abb. 54 – Gruppen-, rollen- und benutzerspezifische Zugriffsrechte

Hinweis: Dieses Beispiel soll lediglich die Auswirkungen der verschiedenen Vorrangsregeln verdeutlichen; es ist nicht als Vorbild für optimal eingestellte Zugriffsrechte gedacht.

6.5 Zugriffsrechte einstellen

Dieser Abschnitt beschreibt den Dialog zum Einstellen der Zugriffsrechte eines Objekts und das Vorgehen zum Ändern der Einstellungen. Der Dialog *Zugriffsrechte* für das aktuelle Objekt (siehe Abb. 55 “Dialog zur Einstellung der Zugriffsrechte” auf Seite 179) wird mit einem Klick auf das Rechtesymbol in der Symbolleiste oder über den Menüpunkt *Ansicht* → *Rechte* aufgerufen.

Nur wenn Sie über das Recht verfügen, die Zugriffsrechte des aktuellen Objekts zu ändern, können Sie Änderungen an den Zugriffseinstellungen vornehmen. Eine solche Änderung der Zugriffsrechte unterliegt – wie jede andere Objektänderung – dem Qualitätssicherungsworkflow, d. h., die Änderung muß der Qualitätssicherung zur Prüfung und Freigabe vorgelegt werden. Lehnt die Qualitätssicherung die vorgelegte Änderung der Zugriffsrechte ab, werden die vorher eingestellten Zugriffsrechte wieder eingesetzt.

Wenn Sie die Zugriffsrechte eines Objekts ändern, beachten Sie bitte folgendes:

- Es muß *mindestens einen* Eintrag in der Liste der Zugriffsberechtigten geben (also einen Benutzer, eine Gruppe, eine Rolle oder den Eintrag “Jeder”). Der letzte vorhandene Eintrag kann nicht gelöscht werden.

- Von den eingetragenen Zugriffsberechtigten muß es mindestens einen geben, der die Erlaubnis hat, die Zugriffsrechte zu ändern. Wenn dieses Recht nur einmal vertreten ist, kann es nicht mehr entzogen und der entsprechende Eintrag nicht gelöscht werden.
- Das Leserecht ist bei allen anderen Zugriffsrechten – mit Ausnahme des Lesens im Produktionssystem – inbegriffen. Wenn Sie einem Benutzer (bzw. einer Gruppe oder Rolle) ein Zugriffsrecht wie Anlegen, Ändern oder Löschen verleihen, erhält er ebenfalls das Leserecht für das Objekt.

Hinweis: Benutzer, die nicht über das Recht verfügen, die Zugriffsrechte des aktuellen Objekts zu ändern, können dennoch den Zugriffsrechte-Dialog aufrufen. Ihnen wird jedoch nur der obere Teil des Fensters angezeigt. Sie können also keine Änderungen vornehmen.

Einen Benutzer (oder anderen Eintrag) hinzufügen

In den folgenden Abschnitten werden die verschiedenen Grundfunktionen zur Einstellung der Zugriffsrechte für das aktuelle Objekt vorgestellt.

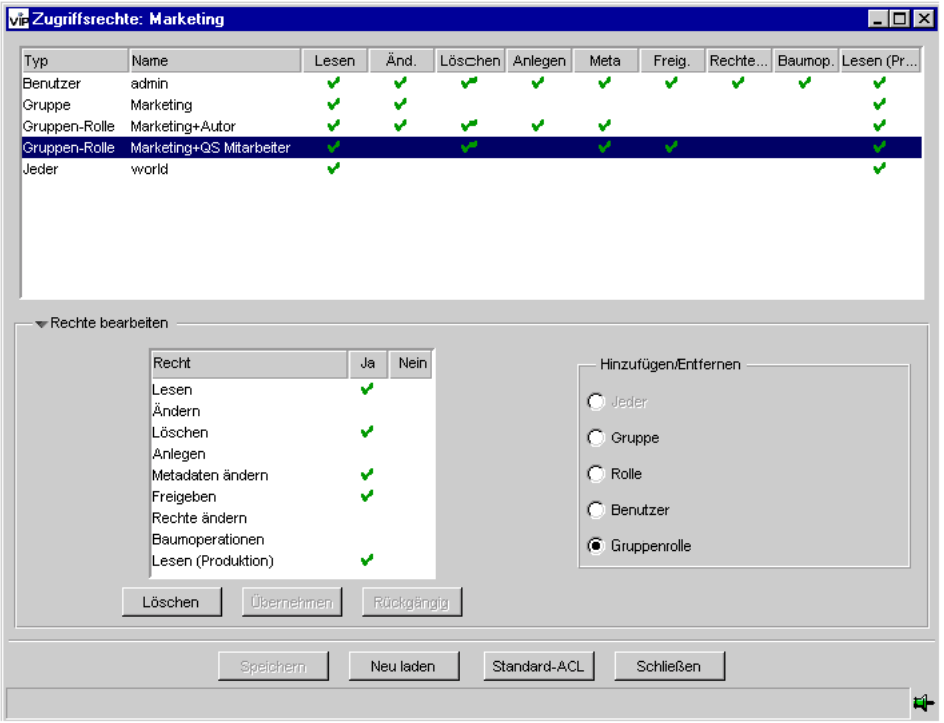

Abb. 55 – Dialog zur Einstellung der Zugriffsrechte

1. Aktivieren Sie im Fensterbereich *Rechte bearbeiten* das gewünschte Optionsfeld:
   - *Gruppe* – um eine Gruppe hinzuzufügen
   - *Rolle* – um eine Rolle hinzuzufügen
   - *Benutzer* – um einen Benutzer hinzuzufügen
   - *Gruppenrolle* – um eine Gruppenrolle hinzuzufügen

   Damit wird der entsprechende Zuordnungsdialog für das Objekt aufgerufen.

> **Hinweis:** Mit der Option *Jeder* werden Zugriffsrechte für alle Benutzer vergeben, die von den anderen Einstellungen nicht betroffen sind (z. B. durch ihre Gruppen- oder Rollenzuordnung).

Abb. 56 – Dialog zum Zuordnen einer Gruppe

2. Markieren Sie in der Liste der verfügbaren Benutzer, Gruppen oder Rollen den gewünschten Eintrag, und klicken Sie auf den *Pfeil nach rechts*.
3. Der Eintrag wird in die Zuordnungsliste auf der rechten Seite übernommen. Klicken Sie auf *Speichern*, um die Zuordnung zu übernehmen und den Zuordnungsdialog zu schließen.
4. Im Dialog *Zugriffsrechte* wird ein entsprechender Eintrag in der Liste der Zugriffsberechtigten eingefügt. Die eingestellten Zugriffsrechte entsprechen zunächst den Standardvorgaben für diesen Benutzer bzw. diese Gruppe oder Rolle. Um die Einstellungen zu ändern, markieren Sie den Eintrag in der Liste, und stellen Sie im unteren Fensterbereich die gewünschten Zugriffsrechte ein.
5. Klicken Sie auf *Speichern*, um die neue Einstellung im System zu speichern.

Einstellen von Zugriffsrechten

1. Um die Zugriffsrechte eines Benutzers auf das aktuelle Objekt einzustellen, markieren Sie den Eintrag in der Liste der Zugriffsberechtigten, und klicken Sie in der Einstellungstabelle auf die gewünschten Zugriffseinstellungen.

   In jeder Zeile der Tabelle kann das entsprechende Recht explizit erlaubt bzw. verboten werden oder unbestimmt bleiben. Beachten Sie dabei, daß

Zugriffsrechte außerdem von gruppen- bzw. rollenspezifischen Einträgen abhängig sind. Siehe Abschnitt 6.4 “Vorrangsregeln” auf Seite 175.

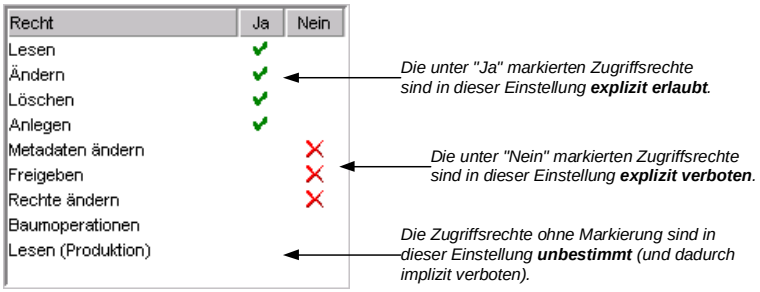

Abb. 57 – Einstellungsmöglichkeiten für einzelne Zugriffsrechte

2. Klicken Sie auf *Übernehmen*, um die Änderungen in der Liste zu übernehmen.
3. Klicken Sie auf *Speichern*, um die neue Einstellung im System zu speichern.

Einen Benutzer aus der Zugriffsliste entfernen

1. Markieren Sie den gewünschten Benutzer in der Liste der Zugriffsberechtigten, und klicken Sie auf *Entfernen*. Der Eintrag wird aus der Liste entfernt.
2. Klicken Sie dann auf *Speichern*, um den Benutzer endgültig zu löschen.

Hinweis: Im Dialog *Zuordnung* haben Sie auch die Möglichkeit, Einträge aus der Zuordnungsliste für das Objekt zu entfernen. Klicken Sie dazu auf das Optionsfeld für die entsprechende Kategorie (Benutzer, Gruppe, Rolle, Gruppenrolle). Damit wird der Dialog *Zuordnung* für diese Kategorie aufgerufen. Dort markieren Sie die gewünschten Einträge in der Zuordnungsliste und klicken dann auf den *Pfeil nach links*. Die markierten Einträge werden aus der Zuordnungsliste entfernt. Anschließend klicken Sie auf *Speichern*, um den Eintrag endgültig zu löschen.

Zugriffsrechte für “alle” Benutzer einstellen

Durch den speziellen Benutzereintrag *Jeder* haben Sie die Möglichkeit, den Zugriff auf ein Objekt für alle Benutzer einzustellen, die von den anderen Einstellungen des Objekts nicht betroffen sind:

1. Sollte es bereits einen Eintrag *Jeder* für das Objekt geben, markieren Sie diesen Eintrag und stellen Sie die gewünschten Zugriffsrechte für alle Benutzer ein.
2. Sollte es für das Objekt noch keinen Eintrag *Jeder* in der Liste der Zugriffsberechtigten geben, fügen Sie diesen Eintrag hinzu, indem Sie im Fensterbereich *Rechte bearbeiten* das Optionsfeld *Jeder* anklicken.
3. Der Eintrag wird der Liste hinzugefügt.
4. Um die Zugriffsrechte auf das aktuelle Objekt anzupassen, markieren Sie den Eintrag in der Liste der Zugriffsberechtigten und stellen Sie die gewünschten Rechte ein.
5. Klicken Sie auf *Speichern*, um die Einstellungen im System zu speichern.

Hinweis: Die Zugriffseinstellung *Jeder* gilt für alle angemeldeten Benutzer, bei denen die Zugriffsrechte auf das Objekt nicht aufgrund eines oder mehrerer anderer Einträge in der Liste der Zugriffsberechtigten festgelegt sind. Haben Sie z. B. einer bestimmten Benutzergruppe den Lesezugriff verboten, können die Mitglieder dieser Gruppe das Objekt nicht lesen, auch wenn die Einstellung *Jeder* den Lesezugriff für alle Benutzer erlaubt.

Zugriffsrechte für das Produktionssystem einstellen

Wie im Pflege- und QS-System kann im VIP’ContentManager auch der Zugriff auf Objekte im Produktionssystem spezifisch geregelt werden.

- **Uneingeschränkter Lesezugriff im Produktionssystem:** Der Lesezugriff im Produktionssystem kann generell – d. h. ohne Anmeldung – erlaubt werden. Dazu stellen Sie für den speziellen Benutzereintrag “Jeder” das Zugriffsrecht “Lesen (Produktion)” als erlaubt ein. Das Objekt kann dann von jedem gelesen werden, der auf das Produktionssystem zugreifen kann. Wenn das Produkti-

onssystem z. B. im Internet verfügbar ist, kann jeder Benutzer des Internets das Objekt ohne Anmeldung in seinem Browser aufrufen.

- **Eingeschränkter Lesezugriff im Produktionssystem:** Wenn der Zugriff auf ein Objekt im Produktionssystem nur eingeschränkt – z. B. nur für bestimmte Benutzergruppen – möglich sein soll, wird das Leserecht nicht für den Eintrag “Jeder” erlaubt, sondern nur für die gewünschten Benutzer, Gruppen oder Rollen. Das Objekt kann dann nur von den berechtigten Benutzern und nach erfolgter Anmeldung gelesen werden.

Grundsätzlich werden auch hier die Zugriffseinstellungen an untergeordnete Objekte vererbt. Nur durch eine Änderung der Zugriffseinstellungen für ein Objekt wird die Vererbungskette unterbrochen. Wenn Sie also für ein bestimmtes Thema Ihrer Website den uneingeschränkten Zugriff im Produktionssystem erlauben, gilt diese Zugriffseinstellung auch für alle untergeordneten Objekte dieses Themas, für die keine eigenen Zugriffsrechte eingestellt worden sind. Siehe auch Abschnitt 6.2 “Vererbung von Zugriffsrechten” auf Seite 171.

Hinweis: Beim Anlegen einer Website wird das Leserecht im Produktionssystem standardmäßig für den speziellen Benutzereintrag “Jeder” erlaubt. Damit wird eine generelle Zugriffserlaubnis auf das Produktionssystem eingestellt. Grundsätzlich gilt jedoch auch im Produktionssystem, daß ein Benutzer erst dann auf ein Objekt zugreifen kann, wenn er über das entsprechende Zugriffsrecht verfügt. Die allgemeine Zugriffserlaubnis können Sie also jederzeit durch eine Änderung der Zugriffsrechte aufheben bzw. beschränken.

Alle objektspezifischen Einstellungen zurücksetzen

Aufgrund der Vererbungsregeln erbt jedes Objekt die Zugriffseinstellungen vom übergeordneten Thema. Die Einstellungen für das Thema können ihrerseits ebenfalls *geerbt* sein. Solange der Zugriff auf das Objekt durch die Einstellungen des Themas zufriedenstellend geregelt ist, braucht das Objekt keine eigenen Zugriffseinstellungen.

Werden die geerbten Zugriffsrechte eines Objekts jedoch verändert, wird die Vererbungskette gebrochen, d. h. Änderungen an den Zugriffseinstellungen des

übergeordneten Themas werden nicht mehr auf die untergeordneten Objekte vererbt.

Sie können jedoch Änderungen an den Zugriffseinstellungen eines Objekts wieder aufheben und damit das Objekt wieder in die Vererbungskette eingliedern, indem Sie im Zugriffsrechte-Dialog auf den Button *Standard-ACL* klicken.

Achtung: Durch Betätigen des Buttons *Standard-ACL* werden sofort sämtliche objektspezifischen Zugriffseinstellungen gelöscht.

6.6 Aufgabenspezifische Zugriffsrechte

In den verschiedenen VIP-Systemen – Pflege, QS und Produktion – sind unterschiedliche Zugriffsrechte erforderlich, um auf Objekte zuzugreifen und sie zu bearbeiten. Die Funktionen des Pflegesystems erfordern insbesondere das *Änderungsrecht*. Die Arbeit im Qualitätssicherungssystem setzt vor allem das *Freigaberecht* voraus. Der Zugriff im Produktionssystem ist auf das Lesen beschränkt und erfordert daher nur das Recht *Lesen im Produktionssystem*.

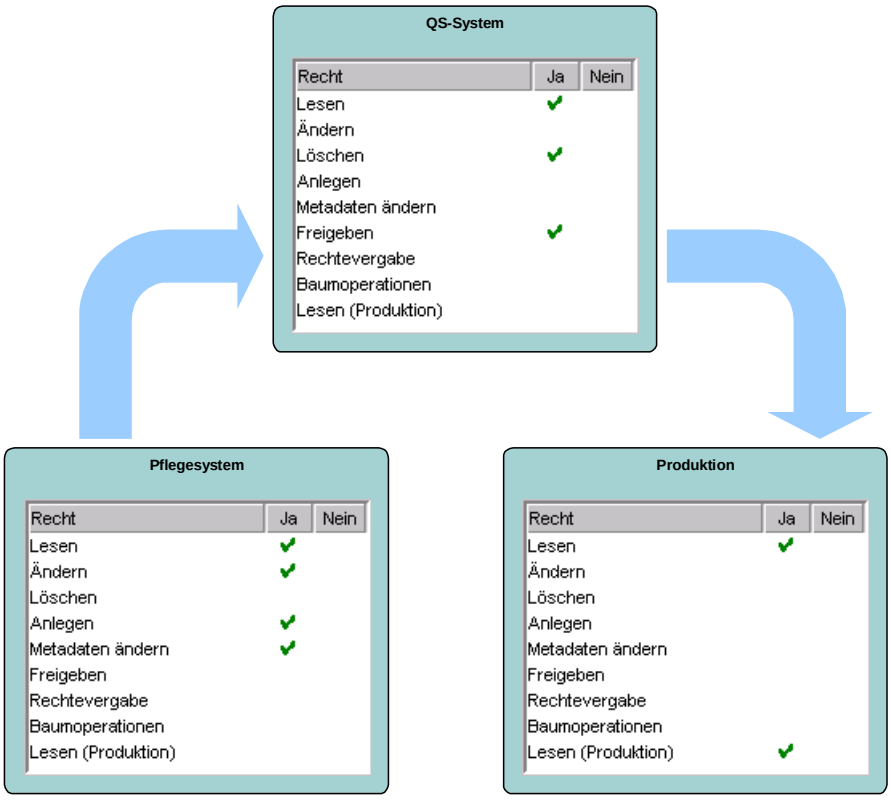

Abb. 58 – Zugriffsrechte für Pflege, QS und Produktion

Die Möglichkeiten eines Benutzers, im Pflegesystem bzw. in der Qualitätssicherung bestimmte Arbeitsschritte an einem Objekt durchzuführen oder das Objekt im Produktionssystem zu lesen, hängen von den Zugriffsrechten des Benutzers auf dieses Objekt ab. So stehen beispielsweise die Funktionen *Ausleihen*, *Zurückgeben* und *Vorlegen* im Pflegesystem nicht zur Auswahl, wenn der Benutzer nicht das Änderungsrecht für das aktuelle Objekt besitzt.

Die folgende Tabelle gibt Ihnen einen Überblick über die Funktionen im Pflege- und Qualitätssicherungssystem und die dafür erforderlichen Zugriffsrechte.

Tabelle 6 – Funktionen und erforderliche Zugriffsrechte

Funktionen	System	erford. Zugriffsrechte
Objekte anlegen	Pflegesystem	Anlegen (auf das übergeordnete Thema)
Ein Objekt *vor* der ersten Freigabe löschen	Pflegesystem	Löschen
Ein Objekt vorlegen	Pflegesystem	Ändern
Ein Objekt bearbeiten (ausleihen, ändern, zurückgeben, vorlegen)	Pflegesystem	Ändern
Metadaten eines Objekts ändern	Pflegesystem	Metadaten ändern
Referenzen eines Objekts ändern	Pflegesystem	Ändern
Ein Objekt umbenennen	Pflegesystem	Metadaten ändern
Ein Objekt ausschneiden	Pflegesystem	Ändern + Baumoperationen
Ein Objekt kopieren	Pflegesystem	Baumoperationen
Ein Objekt einfügen (nach dem Ausschneiden bzw. Kopieren)	Pflegesystem	Anlegen (auf das übergeordnete Thema)
Zugriffsrechte eines Objekts prüfen	Pflegesystem, QS-System	Lesen
Zugriffsrechte eines Objekts ändern	Pflegesystem	Zugriffsrechte ändern
Ein Objekt freigeben bzw. wiedervorlegen	QS-System	Freigeben
Ein Objekt direkt freigeben	Pflegesystem	Ändern
Ein Objekt *nach* der ersten Freigabe löschen	Pflegesystem → QS-System	Löschen + Freigeben

Hinweis: Jeder Zugriff auf ein Objekt setzt das Leserecht voraus. Das Leserecht wird daher automatisch vergeben, wenn einem Benutzer (bzw. einer Gruppe oder Rolle) andere Zugriffsrechte auf ein Objekt eingeräumt werden.

6.7 Benutzer, Gruppen und Rollen

Wie bei einem Netzwerkbetriebssystem können auch im VIP'ContentManager die Benutzer einer Website in Gruppen zusammengefaßt und der Zugriff über die Vergabe von Rechten an diese Gruppen geregelt werden. Bei Bedarf können bestimmte Zugriffsrechte auch an einzelne Benutzer vergeben werden, jedoch wird das in den meisten Fällen die Ausnahme sein. Für viele Organisationen ist die Gruppenbildung und die Bestimmung von Zugriffsrechten über Gruppenrechte ein bewährtes und daher gut übertragbares Prinzip.

Eine Rolle ist – ähnlich wie eine Benutzergruppe – eine Zusammenstellung von Benutzern. Rollen werden aber aufgabenbezogen definiert, während Gruppen in der Regel an organisatorische Strukturen wie Abteilungen oder Projekte geknüpft sind. Je nach Aufgaben können die Rollen in einer Organisation unterschiedlich definiert sein. Einige typische Benutzerrollen, die an der Pflege einer Website beteiligt sein können, sind Redakteure, Grafiker, Projektleiter und QS-Mitarbeiter.

Für eine Rolle können – genauso wie für eine Gruppe – bestimmte Zugriffsrechte auf Objekte definiert werden. Da die Rollen meistens aufgabenbezogen definiert werden, kann die Einstellung von Zugriffsrechten für eine Rolle teilweise noch einfacher sein als für eine Gruppe, da z. B. Redakteure ganz bestimmte Zugriffsrechte wie Anlegen und Ändern brauchen. Die Gruppen haben im Vergleich dazu oft einen thematischen Bezug wie Vertrieb, Marketing, Produktion oder Verwaltung.

Gruppenrollen

Der Zugriff auf ein Objekt kann für eine ganze Gruppe, für eine Rolle oder für die Kombination einer bestimmten Gruppe mit einer spezifischen Rolle eingestellt

werden. Diese Kombination wird als *Gruppenrolle* bezeichnet. Bei der Gruppenrolle handelt es sich nicht um eine Organisationseinheit, die im Administrationssystem definiert wird, sondern um eine Einstellungsmöglichkeit in der Zugriffskontrolle. Das folgende Beispiel verdeutlicht das Konzept der Gruppenrollen:

Angenommen, Sie haben im Administrationssystem mehrere Gruppen sowie die Rollen “Autor” und “QS-Mitarbeiter” definiert. Die Benutzer sind jeweils – ihren Arbeitsbereichen entsprechend – den Gruppen zugeordnet. Die Mitarbeiter des Marketingbereichs gehören also zur Gruppe “Marketing”, die des Bereichs Zentralfunktionen zur Gruppe “Zentralfunktionen” usw. Die Benutzer, die in den jeweiligen Abteilungen für das Erstellen und Pflegen der Objekte zuständig sind, sind der Rolle “Autor” zugeordnet, die Benutzer, die für die Qualitätssicherung der Objekte verantwortlich sind, der Rolle “QS-Mitarbeiter”.

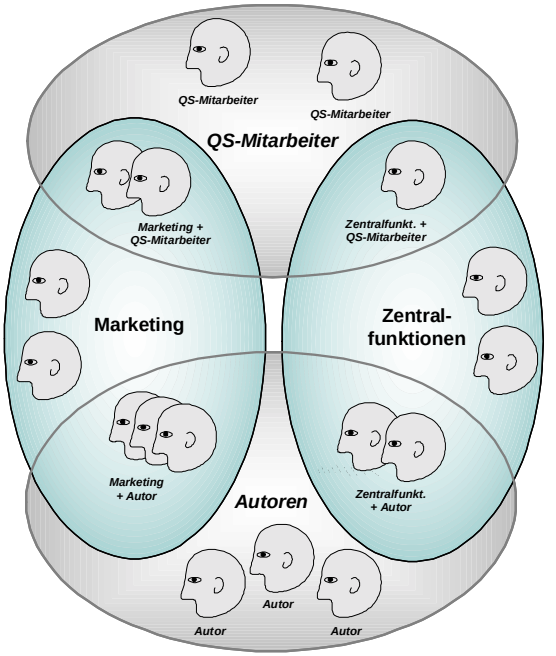

Abb. 59 – Zuordnung von Benutzern zu Gruppen und Rollen

Durch die Verwendung von Gruppenrollen-Einstellungen können die Zugriffsrechte auf Objekte jeweils sehr spezifisch eingestellt werden, nämlich sowohl themenbezogen (durch die Gruppe) als auch aufgabenbezogen (durch die Rolle). Für den Themenbereich Marketing könnten die Zugriffsrechte beispielsweise so eingestellt werden, daß nur die Autoren, die auch der Gruppe “Marketing” zugeordnet sind, über die Rechte “Anlegen”, “Ändern”, “Metadaten ändern” usw. verfügen. Analog könnte das Freigaberecht an die Gruppenrolle “Marketing + QS-Mitarbeiter“ und das Ändern von Zugriffsrechten an die Gruppenrolle “Marketing + Gruppenleiter“ vergeben werden:

Gruppe “Marketing” + Rolle “Gruppenleiter”	Ändern ✓
Gruppe “Marketing” + Rolle “Autor”	Anlegen, Ändern, Metadaten ändern ✓
Gruppe “Marketing” + Rolle “QS-Mitarbeiter”	Freigeben, Löschen ✓

Standardvorgaben für Zugriffsrechte

Im Administrationssystem können für jeden Benutzer sowie für jede Benutzergruppe oder -rolle Standardvorgaben für die Zugriffsrechte festgelegt werden. Wird ein Benutzer (bzw. eine Benutzergruppe oder -rolle) zur Liste der Zugriffsberechtigten eines Objekts hinzugefügt, werden diese Standardvorgaben als Voreinstellungen für die Zugriffsrechte verwendet. Informationen über Standardvorgaben für Zugriffsrechte eines Benutzers (bzw. einer Benutzergruppe oder -rolle) finden Sie in Kapitel 5 “Arbeiten im Administrationssystem”.

Stellvertreter

In der Benutzer-Administration können Sie für jeden Benutzer einen Stellvertreter bestimmen. Der Stellvertreter eines Benutzers kann jederzeit *alle* Funktionen ausüben, zu denen der Benutzer selbst berechtigt ist (vom Zurückstellen eines Objekts bis zum Löschen eines kompletten Themas).

Recht auf Änderung der Zugriffsrechte

Um die Zugriffsrechte eines Objekts zu ändern, muß der Benutzer über das Änderungsrecht für die Zugriffseinstellungen des Objekts verfügen. Dieses besondere Zugriffsrecht sollte nur an ausgewählte Benutzer (bzw. Gruppen oder Rollen) vergeben werden, die mit den Grundlagen der Zugriffskontrolle und dem Zugriffskonzept des Unternehmens vertraut sind.

6.8 Tips

1. **Je einfacher, desto besser!** Je komplexer Sie die Zugriffsregeln gestalten, desto größer ist die Gefahr, daß sie unübersichtlich werden und sich nicht mehr nachvollziehen lassen.
2. Bevor Sie mit der eigentlichen Definition von Zugriffsrechten beginnen, sollten Sie zunächst die Zugriffe analysieren, die in Ihrem Unternehmen notwendig sind:
   - Welche Benutzergruppen gibt es, und auf welche Objekte greifen sie zu?
   - Welche Aufgaben haben die verschiedenen Benutzer?
   - Wer ist an der Erstellung von Website-Inhalten beteiligt?
   - Wer ist für die Qualitätssicherung verantwortlich?
   - Wer legt die Zugriffsrechte fest?
3. Wenn es für ein Objekt oder ein Thema eine allgemeine Regelung gibt, die für (fast) alle Benutzer zutrifft, wie z. B. “alle dürfen die Homepage im Produktionssystem lesen”, ist dies am besten mit einer Einstellung für “Jeder” zu treffen. Die Ausnahmen von dieser allgemeinen Regelung können dann gruppen-, rollen- oder benutzerspezifisch eingestellt werden.
4. Versuchen Sie, spezifische Bereiche zu definieren, in denen der Zugriff durch Erlaubnisse geregelt werden kann. Werden die Zugriffserlaubnisse zu weit gefaßt, muß der Zugriff durch Verbote wieder eingeschränkt werden.

5. Grundsätzlich gilt, daß ein Benutzer erst dann auf ein Objekt zugreifen kann, wenn er über das entsprechende Zugriffsrecht verfügt. Daher sollten explizite Zugriffsverbote mit Vorsicht zugewiesen werden, um den Aufbau von komplexen und unübersichtlichen Zugriffsstrukturen zu vermeiden. Aufgrund der Vorrangsregeln gilt ohnehin ein implizites Zugriffsverbot, da der Zugriff auf ein Objekt nur mit expliziter Erlaubnis möglich ist.

   Selbstverständlich kann es Situationen geben, in denen ein Verbot dennoch sinnvoll ist, etwa um eine generelle Zugriffserlaubnis (“Jeder”) für ganz bestimmte Benutzer oder Gruppen wieder einzuschränken.

6.9 FAQs (Häufig gestellte Fragen)

Baumoperationen

F: Ich möchte ein Thema an eine andere Stelle verschieben. Welche Zugriffsrechte brauche ich, um das zu tun?

A: Das Verschieben besteht aus zwei verschiedenen Operationen, die zusammenhängend durchgeführt werden, nämlich “Ausschneiden” und “Einfügen”. Um ein Objekt zu verschieben benötigen Sie folgende Zugriffsrechte:

- Um das Objekt auszuschneiden, benötigen Sie für dieses Objekt die Rechte “Ändern” und “Baumoperationen”.
- Um das Objekt einzufügen, brauchen Sie das Recht “Anlegen”, und zwar für das Thema, unter dem das Objekt eingefügt werden soll.

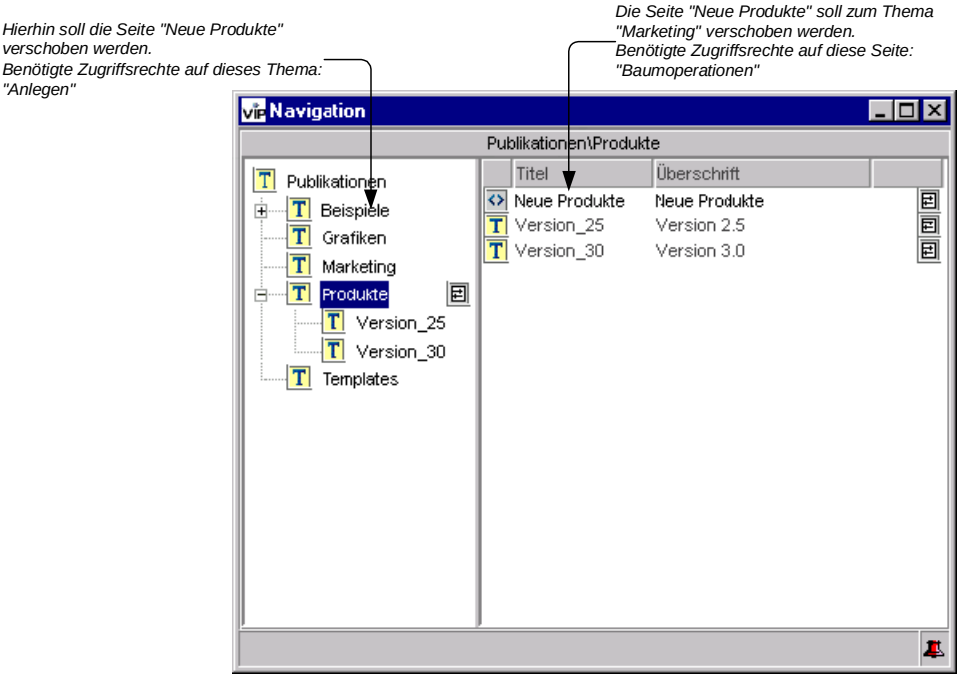

Abb. 60 – Zugriffsrechte zum Verschieben einer Seite

Wenn es sich bei dem zu verschiebenden Objekt um ein Thema handelt, sind für das Themenobjekt die gleichen Zugriffsrechte erforderlich wie beim Verschieben anderer Objekttypen. Die Zugriffsrechte auf untergeordnete Objekte des Themas spielen dabei keine Rolle.

Website-Administratoren

F: Ich habe eine Website angelegt und möchte nun den Website-Administrator bestimmen. Wie kann ich das tun?

A: Den Website-Administrator können Sie nur beim Anlegen der Website festlegen. Wenn Sie keinen Website-Administrator für die Website festgelegt haben, sind die Zugriffsrechte für das Website-Objekt automatisch wie folgt festgelegt:

- Der Benutzer “admin” ist Website-Administrator. Er hat uneingeschränkte Zugriffsrechte auf das Website-Objekt, auch das Recht, die Zugriffsrechte zu ändern.
- Alle anderen Benutzer der Website haben uneingeschränkte Zugriffsrechte auf das Website-Objekt bis auf die Rechte, die Zugriffsrechte zu ändern und Baumoperationen durchzuführen: Dieses hat nur der Benutzer “admin”.

Beachten Sie bitte, daß die Aufgabe bzw. das besondere Zugriffsrecht des Website-Administrators darin besteht, die ersten Themen der Website anzulegen und die Zugriffsrechte auf diese Themen festzulegen. Unterhalb dieser Themen werden neue Objekte von den Benutzern angelegt. Die Zugriffsrechte auf untergeordnete Objekte sind dann vom jeweiligen Thema abgeleitet (entsprechend dem Vererbungsprinzip).

F: Ich habe eine Gruppe mit dem Namen “Website-Administratoren” angelegt und mehrere Benutzer in diese Gruppe aufgenommen. Welche Zugriffsrechte sollen für diese Gruppe eingestellt sein, damit die Benutzer ihre Aufgaben als Website-Administratoren wahrnehmen können?

A: Das besondere Zugriffsrecht des Website-Administrators ist völlig unabhängig von den Einstellungen für Gruppen, Rollen bzw. Benutzer. Die beim Anlegen einer Website als Website-Administrator festgelegten Benutzer haben zunächst uneingeschränkten Zugriff auf diese Website. Sie können unter dem Website-Objekt Themen anlegen, bearbeiten, die Metadaten und die Zugriffsrechte dieser Themen ändern, die Themenbäume verschieben usw. Solange diese Zugriffsrechte nicht – durch Änderung der Zugriffsrechte an einem Thema – wieder entzogen werden, vererben sie sich weiter an die untergeordneten Objekte. In diesem Fall hätte der Website-Administrator auch auf diese untergeordneten Objekte uneingeschränkte Zugriffsrechte.

F: Kann der Website-Administrator neue Benutzer für die Website anlegen?

A: Das Anlegen neuer Benutzer und die Zuordnung von Benutzern zu einer Website sind Funktionen des Administrationssystems. Der Website-Administrator kann daher nur neue Benutzer für die Website anlegen, wenn er im Administrationssystem arbeiten darf. Das ist jedoch von der Auswahl des Benutzers als Website-Administrator völlig unabhängig.

Gruppenrollen

F: Was ist eigentlich eine Gruppenrolle?

A: Eine Gruppenrolle ist die Schnittmenge einer Gruppe und einer Rolle. Wenn Sie z. B. im Administrationssystem eine Gruppe “Marketing” und eine Rolle “Grafiker” definiert haben, dann enthält die Gruppenrolle “Marketing + Grafiker” genau diejenigen Benutzer, die sowohl der Gruppe “Marketing” als auch der Rolle “Grafiker” zugeordnet sind.

F: Ich möchte eine Gruppenrolle definieren. Wie muß ich vorgehen?

A: Gruppenrollen existieren nicht als organisatorische Einheiten im Administrationssystem, sondern werden im Pflegesystem bei der Einstellung von Zugriffsrechten definiert. Im Einstellungsfenster wird ein neuer Eintrag des Typs Gruppenrolle hinzugefügt, für die der Zugriff auf das Objekt eingestellt wird.

F: Wie kann ich einen Benutzer einer Gruppenrolle zuordnen?

A: Für eine Gruppenrolle gibt es keine direkte Benutzerzuordnung, da die Zuordnung aus der *Schnittmenge der Gruppe und der Rolle* ermittelt wird. Diejenigen Benutzer, die sowohl der Gruppe als auch der Rolle zugeordnet sind, verfügen über die für die Gruppenrolle eingestellten Zugriffsrechte.

KAPITEL 7

Arbeiten mit dem VIP'DBC Editor

VIP' stellt umfangreiche Funktionen zum Einbinden von dynamischen Informationen zur Verfügung. Das Einbinden von dynamischen Daten hat den Vorteil, daß zur Laufzeit immer die aktuellsten Informationen aus der Datenbank gelesen werden. Die in der Website angezeigten Informationen, wie z. B. Kundenkarteien, Preislisten, Telefonverzeichnisse, sind somit immer "aktuell", ohne daß die Seiten selbst aktualisiert werden müssen. VIP' unterstützt CSV-, ISAM- und JDBC-Tabellen als Datenquellen und bietet dadurch die Möglichkeit, auf eine Vielzahl von Datenbanken zuzugreifen.

Mit dem VIP'DBC Editor können Sie die Datenquelle und das Erscheinungsbild der Tabelle einstellen. Zu jeder Datentabelle gibt es eine Formattabelle, die das Aussehen der Daten beschreibt und die Sie mit Hilfe des Formattabelleneditors auf einfache Weise bearbeiten können. Mit dem VIP'DBC Editor stellen Sie dem VIP-System eine neue Tabelle zur Verfügung.

> **Hinweis:** Das Einbinden einer VIP'DBC-Tabelle auf einer Seite erfolgt über die JSP-Schnittstelle im VIP'PortalManager.

7.1 Tabellen anlegen und bearbeiten

VIP'DBC Editor starten

Um den VIP'DBC Editor zu starten, melden Sie sich im Pflegesystem der betreffenden Website an, und wählen Sie im VIP-Hauptfenster den Menüpunkt *Anwendungen* → *VIP'DBC* Editor. Beachten Sie bitte, daß dieser Menüpunkt Ihnen

nur zur Verfügung steht, wenn Sie im Administrationssystem dem Funktionsbereich “VIP_DBC_Admin” zugeordnet sind.

Im folgenden ist der VIP’DBC Editor dargestellt:

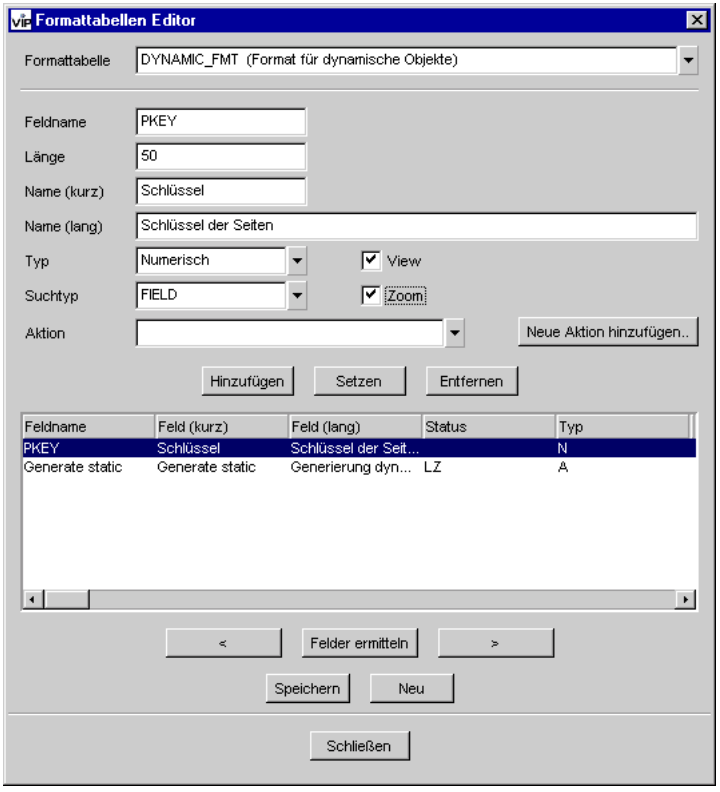

Abb. 61 – Der VIP’DBC Editor

Funktionen

Tabelle neu einbinden

- Klicken Sie im VIP’DBC Editor auf den Button *Neu* und geben Sie den Namen für die neu einzubindende Tabelle ein. Bestätigen Sie mit *OK*.
- Anschließend nehmen Sie die notwendigen Eintragungen im Tabelleneditor-Fenster vor. Klicken Sie auf *Speichern*, um die Eingaben zu bestätigen und damit die Tabelle einzubinden.

Tabelle ändern

- Dazu selektieren Sie die zu ändernde Tabelle im Auswahlfeld *Tabellenliste*, nehmen die Änderungen an den Parametern vor und speichern diese mit Hilfe des Buttons *Speichern*.

VIP’DBC Editor beenden

- Wenn Sie auf den Button *Schließen* klicken, wird der VIP’DBC Editor geschlossen.
- Beachten Sie bitte, daß sich die Tabellen META und OBJEKTE sowie die Formattabellen META_FMT, OBJEKTE_FMT, OBJEKTE_FILTER_FTM und FORMAT nicht verändern lassen. Diese Tabellen werden vom VIP-System zur Datenverwaltung verwendet.

Einstellungen

Im VIP’DBC Editor müssen einige Parameter übergeben werden, um eine Tabelle einzubinden. Dies geschieht über die entsprechenden Felder des Editors, deren Bedeutung im folgenden erklärt wird:

- *Tabellenliste:* In diesem Auswahlfeld können bereits bestehende Tabellen ausgewählt oder durch Eingabe eines Tabellennamens neu erstellt werden.
- *Treiber:* In diesem Auswahlfeld selektieren Sie den Treiber für den Zugriff auf die Tabelle. Der VIP’DBC-Agent unterstützt als Datenquellen CSV-, ISAM- und JDBC-Tabellen.

- *Datenquelle (CSV-Treiber):* Bei CSV-Tabellen müssen Sie den Dateinamen und den vollständigen Pfad in der folgenden Form angeben:

  {verzeichnispfad}|{filename}.csv

  Befindet sich die Tabelle im Verzeichnis **\Tables** oder **\Export_Import** des Pflegeservers der entsprechenden Website, so können Sie über den Button *Suchen* die Datenquelle menügesteuert einfügen. Wird der Pfad nicht angegeben, so wird implizit der Pfad des Tables-Verzeichnisses der ausgewählten Website angenommen.

- *Datenquelle (JDBC-Treiber):* Der Eintrag muß folgende Form haben:

  `{protokoll}:{subprotokoll}:{source};TABLE={Schema}|{Name}`

  Die Voreinstellung für `{protocol}:{subprotocol}` ist jdbc:odbc. Der Datenquellen-Parameter `{source}` muß entsprechend der Datenbankquelle eingetragen werden. `{Schema}|{Name}` kann menügesteuert über den Button *Suchen* angefügt werden, u. U. müssen für diese Aktion bereits die Felder *Benutzer* und *Passwort* ausgefüllt sein, damit ein Zugriff möglich ist. Angaben für `{protokoll}` und `{subprotokoll}` entnehmen Sie bitte der Dokumentation zum verwendeten Datenbanksystem.

- *Typ der Datenquelle (nur JDBC):* Hier müssen die Klasse des JDBC-Treibers und die nötigen Übergabeparameter, getrennt durch Semikolons, aufgelistet werden: `{classname};{prop1}={value};{prop2}={value};....` Diese Angaben sind ebenfalls dem Handbuch des Datenbanksystems zu entnehmen. Wird keine Eintragung in diesem Feld vorgenommen, so wird die JDBC-ODBC-Bridge von Sun benutzt, die durch die Klasse `sun.jbdc.odbc.JdbcOdbcDriver` realisiert wird.

- *Suchen:* Nach Betätigen des Buttons *Suchen* öffnet sich folgender Dialog, in dem Sie eine vorhandene Tabelle auswählen können:

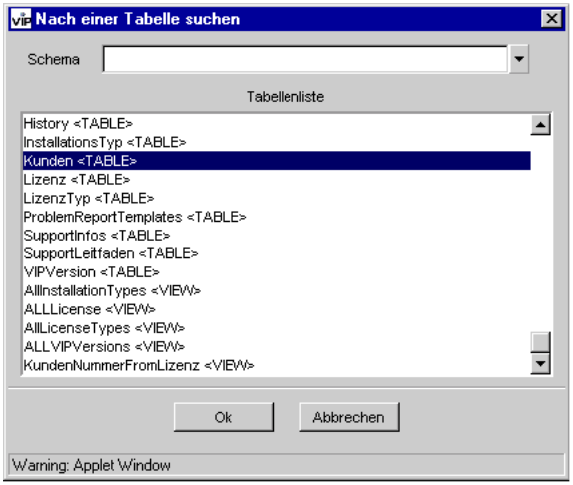

Abb. 62 – Dialog zur Suche nach Tabellen

- *Benutzer, Passwort (nur JDBC):* Falls der Zugriff auf die Datenquelle eine Anmeldung erfordert, tragen Sie hier den Benutzernamen und das Paßwort für das Datenbanksystem ein.
- *Login (nur JDBC):* Mit diesem Optionsfeld aktivieren Sie die Anmeldung an das Datenbanksystem mit dem eingetragenen Benutzernamen und Paßwort.
- *Tabellenname:* Tragen Sie hier den Namen der Tabelle ein. Eine nachträgliche Änderung des Tabellennamens ist nicht möglich.
- *Titel:* Geben Sie hier eine Überschrift für die Tabelle ein.
- *Formattabelle:* Jeder Tabelle wird eine Formattabelle zugeordnet, in der Informationen zur Formatierung der Tabelle enthalten sind. Mit dem Button *Editieren* können Sie eine Formattabelle bearbeiten.
- *Neue Formattabelle / (Formattabelle) Editieren:* Wenn Sie eine neue Tabelle anlegen, können Sie mit einem Klick auf *Editieren* im folgenden Dialog auch eine neue Formattabelle dazu erstellen.

  Wählen Sie hingegen eine bestehende Formattabelle aus der Auswahlliste, können Sie diese mit einem Klick auf *Editieren* bearbeiten.

- *Erster Block:* Dieser Parameter gibt die Nummer des ersten anzuzeigenden Datensatzes der Tabelle an.
- *Anzahl pro Block:* Die Anzahl der anzuzeigenden Datensätze.
- *Schlüssel:* Eines der Tabellenfelder kann als Schlüsselfeld verwendet werden. Dieses Feld muß innerhalb der Tabelle jedoch unbedingt eindeutig sein.
- *Suchfilter:* Hier können Sie eine Suchbedingung eingeben, so daß bereits beim Aufrufen der Tabelle nur die Datensätze angezeigt werden, die der Suchbedingung entsprechen.

  Die Syntax lautet:
  (({feldname} {op} {value}) [|| | &&] ({feldname} {op} {value}) ...)
- *Kopfzeile (nur CSV):* Hier wird die Zeilennummer angegeben, an der die CSV-Tabelle in der Datei positioniert ist. Die erste Zeile einer CSV-Tabelle enthält die Deklaration der Feldnamen. Diese wird als Kopfzeile bezeichnet. In der Regel wird die Kopfzeile am Anfang der Datei stehen, so daß in diesem Feld keine Eintragung erforderlich ist.
- *Speichern:* Mit diesem Button wird die neue bzw. geänderte Tabelle im VIP-System gespeichert.
- *Neu:* Mit diesem Button werden alle nicht gespeicherten Änderungen an der aktuellen (in der Tabellenliste selektierten) Tabelle rückgängig gemacht.
- *Verteilen:* Mit diesem Button wird die aktuelle (in der Tabellenliste selektierte) Tabelle in das QS- und Produktionssystem der Website kopiert.

7.2 VIP'DBC Formattabellen

Den Formattabellen-Editor rufen Sie aus dem VIP'DBC Editor über den Button *Editieren* (bzw. über den darauffolgenden Dialog *Neue Formattabelle*) auf. Hier können Sie die Einstellungen einer Formattabelle bearbeiten sowie neue Formattabellen anlegen.

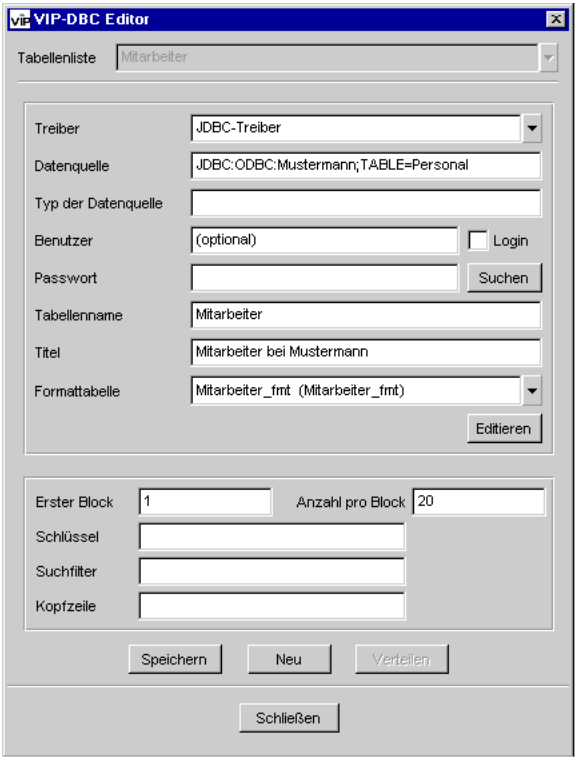

Abb. 63 – Der Formattabellen-Editor

Der Editor ist in zwei Bereiche aufgeteilt: Das Fenster im unteren Teil des Editors dient zur Anzeige sämtlicher Datensätze der Formattabelle, während in den Feldern der oberen Hälfte die einzelnen Einträge des jeweils markierten Datensatzes dargestellt werden. In diesen Feldern werden Änderungen und Neueinträge vorgenommen.

Funktionen

Neue Formattabelle anlegen

Rufen Sie den Formattabellen-Editor über den Button *Editieren* auf. Wenn Sie im VIP'DBC Editor noch keine Formattabelle ausgewählt haben, erscheint der Dialog *Neue Formattabelle*, in den Sie einen Namen für die neue Formattabelle eingeben müssen. Wenn Sie anschließend auf *OK* klicken, erscheint der Formattabellen-Editor.

> **Hinweis:** Wird eine Datenquelle geändert, auf die eine Formattabelle verweist, so ist diese gegebenenfalls anzupassen.

Reihenfolge der Tabelleneinträge ändern

Die Reihenfolge der Datensätze kann beliebig verändert werden. Dazu markieren Sie einen Datensatz und verschieben diesen mit Hilfe der Pfeilbuttons (unterhalb des Fensters) an die gewünschte Position.

Tabelleneinträge hinzufügen und bearbeiten

Mit dem Button *Hinzufügen* wird der Formattabelle ein neuer Datensatz hinzugefügt. Um einen Datensatz zu ändern, markieren Sie den entsprechenden Eintrag, nehmen die gewünschten Änderungen im oberen Teil des Editors vor und bestätigen diese mit einem Klick auf *Setzen*. Mit dem Button *Entfernen* löschen Sie den markierten Datensatz aus der Formattabelle.

Formattabellen-Editor schließen

Über den Button *Speichern* werden die Eintragungen in der Formattabelle gespeichert. Bei Betätigung des Buttons *Schließen* wird der Formattabellen-Editor geschlossen, und Sie befinden sich wieder im VIP'DBC Editor.

Anlegen einer weiteren Formattabelle

Klicken Sie auf den Button *Neu*: Es öffnet sich ein Dialog, in dem Sie den Namen der neu anzulegenden Formattabelle angeben können. Klicken Sie

dann auf *OK*, um die neue Formattabelle anzulegen. Diese können Sie anschließend im Formattabellen-Editor bearbeiten.

Formattabelle verteilen

Dazu selektieren Sie die zu verteilende Formattabelle im Auswahlfeld *Formattabelle*. Wenn Sie anschließend auf den Button *Verteilen* klicken, wird die Formattabelle in das QS- und Produktionssystem kopiert und ist dann auch dort verfügbar. Eventuell müssen in der Metatabelle noch Pfade angepaßt werden.

Mögliche Einstellungen

Im folgenden werden mögliche Einstellungen beschrieben, bei denen die entsprechenden Werte aus der Formattabelle herausgelesen und darauf basierende Aktionen bzw. Darstellungen auf einer JSP-Seite erzeugt werden können.

Es besteht die Möglichkeit, der Formattabelle genaue Angaben über die Art und Formatierung der einzelnen Felder einer Tabelle zuzuweisen. Folgende Felder gibt es:

- *Feldname:* Durch diesen Eintrag kann die Zuordnung der Tabellenspalte (Datenfelder) mit den Zeilen (Datensätzen) dieser Formattabelle vorgenommen werden.

  Hinweis: Die Eintragungen in diesem Feld dürfen keine Sonderzeichen enthalten.

- *Länge der Spalte:* Gibt die Breite der Spalte in Pixeln an.
- *Name (kurz):* Diese Kurzbezeichnungen werden als Spaltenüberschriften der Tabelle benutzt.
- *Name (lang):* Ausführliche Beschreibung der Tabellenspalte.
- *View und Zoom (Optionsfelder):* Durch Aktivieren dieser Optionsfelder können die Flags L und Z (unabhängig voneinander) gesetzt werden.

- *Typ:* Hiermit wird die Art des Feldinhaltes festgelegt. Mögliche Einstellungen sind:

Typ (im Auswahlfeld)	Entsprechung in der Formattabelle
Alpha-Numerisch	A
Numerisch	N
Datum	D
Zeit	T
Zeitstempel	DT

- *Suchtyp:* Hiermit wird der Suchtyp für dieses Feld (normalerweise FIELD) angegeben. Das bedeutet, daß innerhalb des Feldes nach dem Suchbegriff gesucht werden kann. Die anderen beiden Suchtypen DOC und FILE beziehen sich auf die Suche von Dateien, die innerhalb des Feldes angegeben werden. Dies bedeutet, es wird nicht der Feldinhalt durchsucht, sondern dieser wird als Datei interpretiert, und die wiederum wird durchsucht. Dabei wird davon ausgegangen, daß DOC eine absolute Pfadangabe und FILE eine relative Pfadangabe zum Verzeichnis des entsprechenden VIP-Servers erwartet.
- *Aktion:* Mit diesem Feld kann einer Spalte eine Aktion zugeordnet werden. Diese Option stellt für den Anwender der Website ein Instrument zur Interaktion mit dem System bereit. Sie können einer Tabellenspalte z. B. folgende Aktionsattribute zuordnen, die in der Formattabelle gespeichert werden und beim Einbinden der Tabelle über die JSP-Schnittstelle im VIP'PortalMananger (Vip'DBCBean) berücksichtigt werden können:
  - *EMAIL:* Die Eintragungen dieser Spalte werden als E-Mail-Adressen interpretiert.
  - *GROUP_EMAIL:* Alle Eintragungen in dieser Spalte werden als Empfänger für eine E-Mail interpretiert.

- *TABLE:* Die Felder dieser Spalte enthalten den Namen anderer Tabellen, die beim Ausführen dieses Aktionsattributs über den VIP'PortalManager dargestellt werden können.
- *VERWEISE:* Jede Spalte kann auf eine andere Spalte verweisen. Um einen solchen Verweis zu erzeugen, wird aus dem Auswahlfeld *Aktion* der Spaltenname ausgewählt, auf den verwiesen werden soll. Im folgenden Dialog wird z. B. von der Spalte "Informationsabruf" auf die Spalte "General" verwiesen.

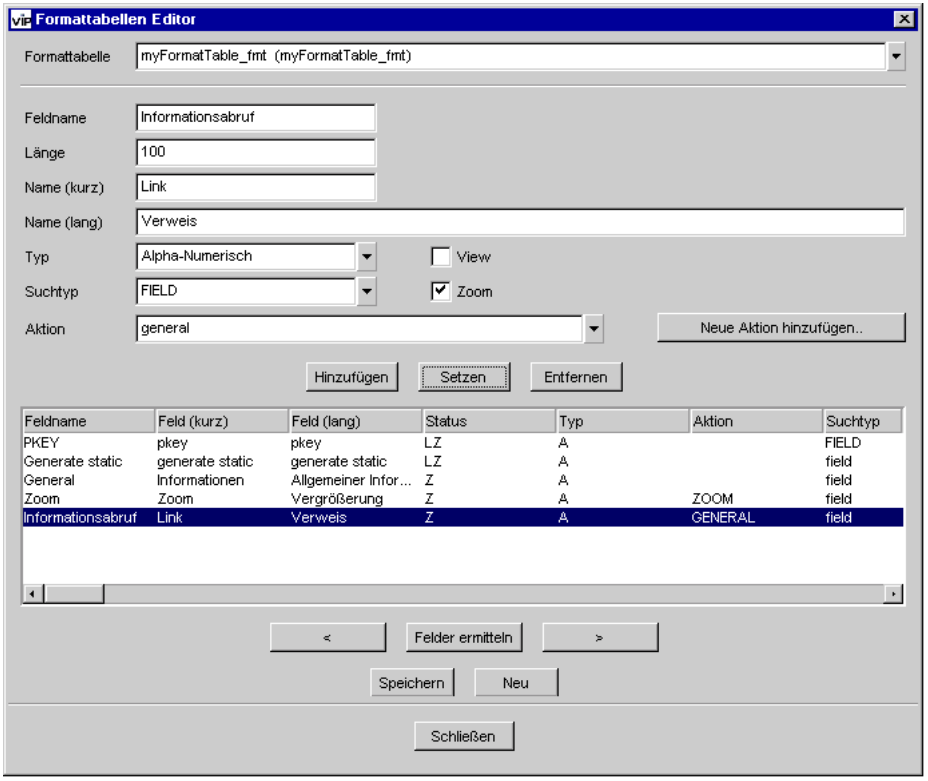

Abb. 64 – Verweis auf eine andere Spalte im Formattabellen-Editor

Zusätzlich zu diesen standardisierten Typen können eigene dynamische Aktionsattribute hinzugefügt werden. Über den Button *Neue Aktion hinzufügen* kann in einer Spalte ein eigenes dynamisches Aktionsattribut hinterlegt werden.

ANHANG A

DefaultContent-Agent

Der DefaultContent-Agent bietet die Möglichkeit, mit den Seitenvorlagen einer Website bestehende VIP-Objekte als Inhaltsvorlagen zu verknüpfen und dadurch den Standardinhalt von neu angelegten Objekten vorzugeben. Damit kann beim Anlegen einer HTML-Seite (oder eines Themas) automatisch der Inhalt eines bestehenden VIP-Objekts in das neue Objekt übernommen werden.

Die Funktionsweise des DefaultContent-Agenten wird über eine Konfigurationsdatei konfiguriert. Es kann für jede Vorlage einer Website eine Inhaltsvorlage mit dem Standardinhalt für die darauf basierenden Objekte erstellt werden. Durch die Einstellungen in der Konfigurationsdatei werden die Vorlagen der Website mit den Inhaltsvorlagen verknüpft.

Wird eine neue HTML-Seite (Objekttyp “HTML” oder “Thema”) im Pflegesystem angelegt, wird vom DefaultContent-Agenten überprüft, ob die gewählte Vorlage mit einer Inhaltsvorlage verknüpft ist. Wenn ja, wird der Inhalt aus der Inhaltsvorlage in das neue Objekt eingefügt.

Die Funktion des DefaultContent-Agenten, beim Anlegen von neuen Objekten den Inhalt einer vordefinierten Inhaltsvorlage einzufügen, hängt von mehreren Bedingungen ab. Diese werden automatisch durch den DefaultContent-Agenten geprüft, wenn ein Benutzer im Pflegesystem ein neues Objekt anlegt:

- Ist der Typ des neuen Objekts “HTML” oder “Thema”? Nur für diese beiden Objekttypen kann ein Standardinhalt definiert werden.
- Wurde für das neue Objekt eine Datei als Inhalt gewählt (*Neu aus Datei*)? In diesem Fall wird nicht der Standardinhalt (aus der Inhaltsvorlage), sondern der Inhalt der gewählten Quelldatei eingefügt.
- Ist die gewählte Vorlage des neuen Objekts in der Konfigurationsdatei **DefaultContent.properties** mit einer Inhaltsvorlage verknüpft?

- Wenn der Seitenvorlage eine Inhaltsvorlage zugewiesen ist: Existiert die eingestellte Inhaltsvorlage tatsächlich als HTML-Seite (Objekttyp “HTML” oder “Thema”) in der Website?

Nur wenn alle Vorbedingungen erfüllt sind, fügt der DefaultContent-Agent den entsprechenden Standardinhalt in die neue HTML-Seite ein.

A.1 Konfiguration

Bei der Installation des VIP’ContentManager (ab Version 5e.03) wird die im folgenden dargestellte Konfigurationsdatei

{VIP_Installationsverzeichnis}\edit\config\viptools\DefaultContent\ DefaultContent.properties

automatisch angelegt. In dieser Datei stellen Sie die Verknüpfungen zwischen den Seitenvorlagen und den Inhaltsvorlagen ein.

```
#
# Default Value
#
DebugMode=Off
#
# Following entries assign a VIP default content (example: OID 211)
# to a VIP template (example: OID 201).
# The website has to be considered.
#
# [website name]
# 201=211
#
# Please add your entries for your website here:
```

Die Datei **DefaultContent.properties** enthält am Anfang eine globale Einstellung, die für alle Websites gültig ist:

- `DebugMode`: Diese Einstellung kann den Wert `On` oder `Off` besitzen. `On` bewirkt das Protokollieren interner Variablen von Default Content in die Log-Datei **log.out** des Edit-Server, die sich im Verzeichnis

{VIP-Installationsverzeichnis}\edit befindet. `Off` unterbindet diese Ausgaben. Die Standardeinstellung ist `Off`.

Desweiteren enthält die Datei website-spezifische Angaben, die jeweils in einer mit dem Namen der Website gekennzeichneten Sektion stehen:

- Sektionsüberschrift: `[{Website-Name}]`
  In jeder Sektionsüberschrift geben Sie den Namen der Website (in eckigen Klammern) an, für die die Sektionseinstellungen gelten.
- Zuweisungen: `{Objekt-ID Vorlage} = {Objekt-ID Inhaltsvorlage}`
  Verknüpfung einer Vorlage mit einem Objekt der Website als Inhaltsvorlage (Default Content). Hier sind jeweils die entsprechenden Objekt-IDs der Vorlage und der Inhaltsvorlage einzutragen.

Die Einträge einer Sektion gelten nur für die in der Sektionsüberschrift genannte Website.

Für den Einsatz des DefaultContent-Agenten muß dieser registriert werden. Dazu ist folgender Eintrag in der Konfigurationsdatei **{VIP-Installationsverzeichnis}\edit\config\serverAgents.properties** zu machen:

```
de.gauss.vip98.user.DefaultContent.DefConServerAgent:
```

Hinweis: Nach erfolgtem Eintrag muß der Edit-Server neu gestartet werden, damit die Einstellung übernommen wird.

A.2 Arbeiten mit dem DefaultContent-Agenten

Der DefaultContent-Agent benutzt VIP-Vorlagen und gewöhnliche VIP-Objekte, um den leeren Inhalt eines neuen Objekts durch den Inhalt eines bestehenden Objekts (der Inhaltsvorlage) zu ersetzen. Folgender Ablauf ist denkbar, um in einem bestimmten Thema einer Website alle neuen (HTML-) Seiten mit einem Default Content zu versehen.

Das folgende Beispiel zeigt, wie Sie von Beginn an vorgehen sollten, um mit Default Content zu arbeiten.

1. Starten Sie das Pflegesystem, und öffnen Sie die gewünschte Website, z. B. “Mustermann”.
2. Im Thema “Templates” (bzw. einem darunterliegenden Thema) legen Sie die zu verknüpfenden Vorlagen an. Für unser Beispiel arbeiten wir mit den Vorlagen “Projektbericht” (Objekt-ID 201) und “Projektdokumentation” (Objekt-ID 202).

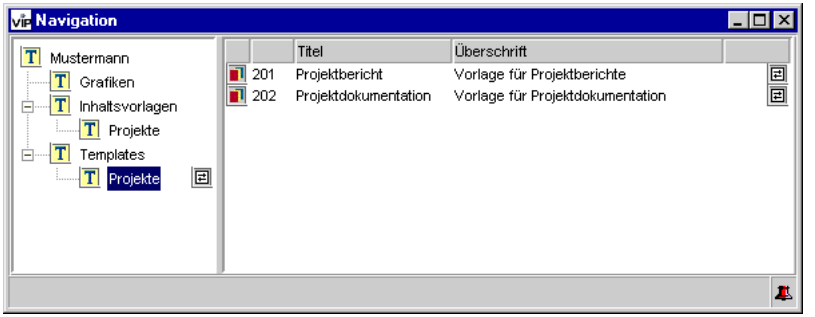

Abb. 65 – Vorlagen im Thema “Templates/Projekte”

3. Legen Sie in der Website ein Thema zur Organisation der Inhaltsvorlagen an. In unserem Beispiel arbeiten wir mit dem Thema “Inhaltsvorlagen”.
4. Im Thema “Inhaltsvorlagen” (bzw. einem darunterliegenden Thema) legen Sie entsprechende HTML-Seiten mit den Standardinhalten für die beiden Vorlagen “Projektbericht” und “Projektdokumentation” an. Für unser Beispiel arbeiten wir mit den HTML-Seiten “Projektbericht” (Objekt-ID 211) und “Projektdokumentation” (Objekt-ID 212).

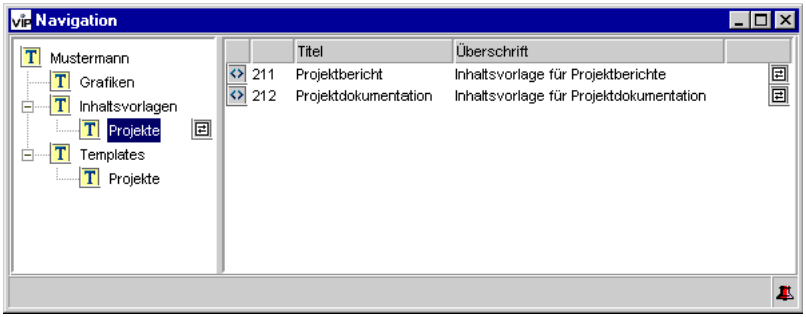

Abb. 66 – Inhaltsvorlagen im Thema “Inhaltsvorlagen/Projekte”

> **Hinweis:** Es wird empfohlen, sich die OIDs sowohl der Seitenvorlage als auch der Inhaltsvorlage zu notieren, da der DefaultContent-Agent nur korrekt arbeiten kann, wenn die OIDs in der Konfigurationsdatei richtig zugeordnet wurden. Sie ermitteln die OID eines Objekts, indem Sie links neben der *Titel*-Spalte mit gedrückter Maustaste die ansonsten verborgene Spalte für die OID aufziehen.

5. Stellen Sie in der Konfigurationsdatei

   {VIP_Installationsverzeichnis}\edit\config\viptools\DefaultContent\DefaultContent.properties

   die Verknüpfungen zwischen den Seitenvorlagen und den Inhaltsvorlagen ein.

   In der Konfigurationsdatei fügen Sie eine Sektion mit dem Namen der Website – also “Mustermann” – als Sektionsüberschrift ein. Darunter fügen Sie für jede Verknüpfung zwischen einer Seitenvorlage und einer Inhaltsvorlage eine Zeile mit den entsprechenden Objekt-IDs (verbunden mit dem Zeichen “=”) ein:

   ```
   [{Website-Name}]

   {Objekt-ID der Vorlage}={Objekt-ID der Inhaltsvorlage}
   ```

   Die Einstellungen für unser Beispiel würden dann so aussehen:

```
[Mustermann]
201=211
202=212
```

6. Wenn Sie die Einstellungen in der Konfigurationsdatei vorgenommen haben, starten Sie den Edit-Server neu, damit die Einstellungen übernommen werden.
7. Legen Sie nun in dieser Website eine neue HTML-Seite (Objekttyp “HTML” oder “Thema”) an, und wählen Sie dabei eine der entsprechenden Vorlagen. Es wird dann automatisch der Inhalt aus der verknüpften Inhaltsvorlage in die neue Seite kopiert.

ANHANG B

HTMLConverter-Agent

Eine wichtige Funktion von Web Content Management Systemen ist die Verarbeitung von Quelldateien, die nicht im HTML-Format vorliegen. Der VIP'ContentManager erfüllt diese Funktion im wesentlichen mit Hilfe des Objekttyps Verbundobjekt. Dieser Objekttyp repräsentiert komplexe Dokumentstrukturen, die als ein Dokument verwaltet werden, z. B. wenn mit Hilfe eines Konverters aus Textverarbeitungsdokumenten ein Satz von HTML-Seiten generiert wurde. Der Objekttyp Verbundobjekt speichert solche Quelldateien zusammen mit den generierten Dateien ab.

Ab der Version 5e verfügt der VIP'ContentManager über einen integrierten HTMLConverter-Agent, der die Anbindung an ein externes Konvertierungsprogramm realisiert. Somit ist es möglich, Konvertierungen automatisch vom System ausführen zu lassen. Die VIP-Umgebung muß nicht mehr verlassen werden.

> **Hinweis:** Das externe Konvertierungsprogramm zählt **nicht** zum Lieferumfang des VIP'ContentManager.

Der vorliegende Anhang behandelt in den folgenden beiden Abschnitten die Installation der für den Einsatz des HTMLConverter-Agent notwendigen Komponenten sowie deren Konfiguration. Anschließend wird die Funktionsweise des automatischen Konvertierungsprozesses dargestellt. Im letzten Abschnitt wird ein Programm vorgestellt, mit dem die Konfiguration unabhängig vom VIP'ContentManager getestet werden kann.

B.1 Installation

Für den Einsatz des HTMLConverter-Agent ist die Installation eines entsprechenden Konvertierungsprogramms erforderlich. Anschließend muß der HTMLConverter-Agent an der API des Edit-Servers registriert werden.

Installationsvoraussetzungen

- Installation des VIP'ContentManager in der Version 3.08 oder höher,
- Zugriffsrecht auf das Pflegesystem,
- Verfügbarkeit eines externen Konvertierungsprogramms.
  Verwendet werden können grundsätzlich solche Programme, die auf demselben Betriebssystem einsatzfähig sind, auf dem der Edit-Server läuft, über eine Kommandozeilenschnittstelle aufgerufen und nach erfolgter Konvertierung automatisch beendet werden können.

Installation des Konvertierungsprogramms

Die Installation und Konfiguration des Konvertierungsprogramms richtet sich nach den Angaben des jeweiligen Herstellers. Es muß auf demselben System installiert werden, auf dem auch der Edit-Server des VIP'ContentManager installiert ist.

Einstellungen für den Einsatz des HTMLConverter-Agent

Zunächst erfolgt die Registrierung des Agenten. Dazu muß ein Eintrag in der Datei **serverAgents.properties** im Konfigurationsverzeichnis des Edit-Servers vorgenommen werden. Die Standardeinstellung in dieser Datei lautet wie folgt:

```
# de.gauss.vip98.user.HTMLConverterAgent.HTMLConverterAgent:➪
  <website1> <website2>...
```

Zum Einsatz des HTMLConverter-Agent muß dieser aktiviert und die Datei **serverAgents.properties** entsprechend angepaßt werden. Zur Aktivierung des HTMLConverter-Agent ist das Doppelkreuz am Anfang der Zeile zu entfernen. Weiterhin ist der Eintrag `<website1>` anzupassen. Er entspricht dabei dem Namen einer Website, auf die der Agent registriert wird. Es können mehrere, durch Leerzeichen separierte Website-Namen zur automatischen Konvertierung registriert werden. Das folgende Beispiel zeigt, wie die Datei **serverAgents.properties** nach erfolgter Aktivierung und Anpassung aussehen könnte:

```
de.gauss.vip98.user.HTMLConverterAgent.HTMLConverterAgent:Mustermann
```

Nach Eingabe der Änderungen muß der Edit-Server neu gestartet werden, damit die Einstellungen übernommen werden.

B.2 Konfiguration

Die Einträge zur Konfiguration des HTMLConverter-Agent werden in der Datei **converter.properties** vorgenommen, die sich in dem Konfigurationsverzeichnis des Edit-Servers befindet. In dieser Datei können die folgenden Parameter gesetzt werden. Dabei ist für alle Namen auf die exakte Groß- und Kleinschreibung zu achten. Die Standardwerte sind hier durch Unterstreichen gekennzeichnet.

Tabelle 7 – Einträge in der Datei converter.properties

Schlüssel	Optional	Wert	Erläuterung
`tempDir`	Ja	Verzeichnis der Zieldatei	Angabe eines temporären Basis-Verzeichnisses, in dem die Konvertate abgelegt werden sollen. Name und Pfad des Verzeichnisses müssen angegeben werden. Beispiel: tempDir = c:\\Temp\\Converter\\Output
`tempDirUseSubdir`	Ja	true | false	Angabe, ob die Konvertate in einem Unterverzeichnis des Basis-Verzeichnisses abgelegt werden sollen. Zu diesem Zweck ist der Wert `true` anzugeben. Beispiel: `tempDirUseSubdir = true`
`tempDirRemove`	Ja	true | false	Angabe, ob das angelegte Unterverzeichnis nach Abschluß der Konvertierung gelöscht werden soll. Wird nur dann verwendet, wenn Unterverzeichnisse des Basis-Verzeichnisses verwendet werden (tempDirUseSubdir = true). Beispiel: `tempDirRemove = true`

Schlüssel	Optional	Wert	Erläuterung
`validExtensions`	Nein	Leerzeichen-separierte Liste von Dateityp-endungen	Es können unterschiedliche Ausgangsformate durch je eigene Konvertierungs-programme bedient werden. Eine Liste der zulässigen Formate in Form der Dateiendungen ist anzugeben. Beispiel: `validExtensions = doc xls txt`
`timeout`	Nein	Millisekunden	Zeit in Millisekunden, die ein Konvertierungsvorgang maximal andauern soll. Bei Überschreitung wird die Konvertierung abgebrochen und eine entsprechende Fehlermeldung generiert. Beispiel: `timeout = 5000`
`synchronizedConvert`	Ja	true | false	Angabe, ob die Konvertierung synchronisiert, d. h. sequentiell durchgeführt werden soll. So kann sichergestellt werden, daß zu einem bestimmten Zeitpunkt stets nur eine Konvertierung vollzogen wird. Beispiel: `synchronizedConvert = true`

Schlüssel	Optional	Wert	Erläuterung
`maxSourceFileLength`	Ja	Byte	Maximale Größe einer Quelldatei in Byte. Default ist 10000000. Bei Überschreitung dieser Größe wird die Konvertierung mit Ausgabe einer Fehlermeldung abgebrochen. Beispiel: `maxSourceFileLength = 2000000`
`secureConvert`	Ja	true | false	Angabe, ob mit einer Sicherheitskopie gearbeitet werden soll. Dies kann nur dann erfolgen, wenn die Konvertate in einem Unterverzeichnis des Basis-Verzeichnis gespeichert werden (`tempDirUseSubdir = true`). In diesem Fall wird die Quelldatei in das temporäre Verzeichnis kopiert. Beispiel: `secureConvert = true`
`debugOn`	Ja	true | false	Angabe, ob die Arbeitsschritte des Konverters protokolliert werden sollen. Es werden Informationen zur Analyse von evtl. auftretenden Problemen während des Konvertierungsvorgangs geliefert. Beispiel: `debugOn = true`

Der Eintrag `validExtensions` bedarf noch zusätzlicher Angaben, die im folgenden aufgeführt werden:

Tabelle 8 – Zusätzliche Angaben für den Eintrag `validExtensions`

Schlüssel	Erläuterung
`{extension}.converterClassName`	Der voll qualifizierte Name der Klasse, die das jeweilige Format konvertiert. Beispiel: `doc.converterClassName = ⇨ de.gauss.vip98.user.⇨ HTMLConverterAgent.ExeFileConverter`
`{extension}.arg1`	Das erste Argument für die jeweilige Klasse inklusive Pfad. In der Regel handelt es sich um eine exe-Datei. Beispiel: `doc.arg1 = c:\\wcvt32.exe`
`{extension}.arg2`	Das zweite Argument für die jeweilige Klasse. In der Regel handelt es sich um die Parameter der Klasse. In diesem Eintrag können Platzhalter verwendet werden, die zur Laufzeit ersetzt werden. Diese Platzhalter sind: `[-SRC-]`: Absoluter Pfad zur Quelldatei `[-TARGET-]`: Absoluter Pfad zur Zieldatei `[-TARGETPATH-]`: Pfad zur Zieldatei ohne Dateiname `[-TARGETNAME-]`: Name der Zieldatei ohne Pfad Beispiel: `doc.arg2 = [-SRC-] [-TARGET-]`

Schlüssel	Erläuterung
`{extension}.env1`	Optionaler Parameter. Beschreibt eine Environment-Variable, die für die Konvertierung gesetzt werden soll. Das Format dieser Variablen ist `{key}={value}`. Beispiel: `doc.env1 = PATH=C:\\WINNT`
`{extension}.env2`	Eine zweite optionale Environment-Variable. Es können n solcher Variablen gesetzt werden, soweit das Suffix lückenlos hochgezählt wird. Beispiel: `doc.env2 = TEMP=C:\\TEMP`

Hinweis: Die Konfiguration sollte zunächst außerhalb der VIP'ContentManager-Umgebung mit Hilfe des beigefügten Testprogramms geprüft werden. Nach erfolgreichem Test kann die dort verwendete Konfigurationsdatei ohne weiteres für den Einsatz im Edit-Server genutzt werden. Zu diesem Zweck muß die Datei aus dem Testverzeichnis in das Konfigurationsverzeichnis des Edit-Servers kopiert werden.

Die folgende Beispieldatei zeigt, wie die Konfigurationsdatei **converter.properties** aussehen könnte. Dabei ist zu beachten, daß in dieser Konfiguration die erzeugten Konvertate nicht von der Festplatte entfernt werden, da der Parameter `tempDirRemove` nicht gesetzt ist. In diesem Fall sollte der Administrator die Konvertate gelegentlich manuell entfernen, da ansonsten die Kapazität der Festplatte unnötig belastet wird.

```
tempDir = c:\\Temp\\converterTest
validExtensions = doc
timeout = 8000
maxSourceFileLength = 10000000
doc.converterClassName =
   de.gauss.vip98.user.HTMLConverterAgent.ExeFileConverter
doc.arg1 = D:\\Programme\\WebConvertPro\\wcvt32.exe
doc.arg2 = [-SRC-] [-TARGET-] HTML
   D:\\Programme\\WebConvertPro\\styles\\webconvert2.cfg
doc.env1 = PATH=C:\\WINNT\\system32;C:\\WINNT
doc.env2 = TEMP=C:\\TEMP
```

Der HTMLConverter-Agent schreibt seine Initialisierungs-Parameter in die Protokolldatei des Edit-Servers. Diese Einträge sehen für die oben angegebene Konfiguration wie folgt aus. Zu beachten ist dabei, daß neben den aufgeführten Einträgen weitere existieren können, die von anderen System-Prozessen stammen.

```
...
Folgender Server-Agent wurde gestartet:
- Hersteller:     Gauss Interprise AG
- Beschreibung:   HTMLConverterAgent
- Version:        Version 1.0
- Ab VIP-Version: 3.0
...
HTMLConverterAgent: Agent registered for website Mustermann.
HTMLConverterAgent: Agent registered for EVENT_CREATED and
EVENT_CHECKED_IN.
HTMLConverterAgent: Target extension is htm.
HTMLConverterAgent: Processing is asynchron.
HTMLConverterAgent: Agent processes compound if AutoGenerated = ➪
  autogenerated;.
HTMLConverterAgent: Init: Output will be placed in c:\Temp\converterTest.
HTMLConverterAgent: Init: Separate subdirectories will be used for each ➪
  conversion.
HTMLConverterAgent: Init: Separate subdirectories will not be removed  ➪
  after conversion.
HTMLConverterAgent: Init: Source file will be copied to working directory.
HTMLConverterAgent: Init: No source files will be converted with  ➪
  length > 10000000.
HTMLConverterAgent: Init: Converter tool will not be called in multi➪
  threaded mode.
HTMLConverterAgent: Init: Conversion timeout is 8000 milliseconds.
HTMLConverterAgent: Init: Extension found: doc.
HTMLConverterAgent: Init: Converter class for doc: ➪
  de.gauss.vip98.user.HTMLConverterAgent.ExeFileConverter.
HTMLConverterAgent: Init: arg1 for doc: ➪
  D:\Programme\WebConvertPro\wcvt32.exe.
HTMLConverterAgent: Init: arg2 for doc: [-SRC-] [-TARGET-] HTML ➪
  D:\Programme\WebConvertPro\styles\webconvert2.cfg.
HTMLConverterAgent: Init: doc.env1 for doc:
PATH=C:\WINNT\system32;C:\WINNT.
HTMLConverterAgent: Init: doc.env2 for doc: TEMP=C:\TEMP.
```

Neben den aufgeführten Einträgen werden pro Konvertierungsvorgang weitere Einträge generiert. Diese sehen wie folgt aus:

```
...
HTMLConverterAgent: Processing object TestDocument
HTMLConverterAgent: [TestDocument] Start external converter process for ⇨
  D:\vipsysteme\vip5e\edit\jco\WebSite\a\a15\_betriebsordnung-cd.doc...
HTMLConverterAgent: Converting to directory c:\Temp\converterTest\5540
HTMLConverterAgent: secureConvert is enabled -> copying ⇨
  D:\vipsysteme\vip5e\edit\jco\WebSite\a\a15\_betriebsordnung-cd.doc to ⇨
     c:\Temp\converterTest\5540\_betriebsordnung-cd.doc
HTMLConverterAgent: Running D:\Programme\WebConvertPro\wcvt32.exe
   c:\Temp\converterTest\5540\_betriebsordnung-cd.doc
   c:\Temp\converterTest\5540\betriebsordnung-cd.html HTML
   D:\Programme\WebConvertPro\styles\webconvert2.cfg
HTMLConverterAgent: [TestDocument] External converter processed finished.
   Converted c:\Temp\converterTest\5540\_betriebsordnung-cd.doc to ⇨
    c:\Temp\converterTest\5540\betriebsordnung-cd.html
HTMLConverterAgent: [TestDocument] Now updating MetaData ...
HTMLConverterAgent: [TestDocument] import-pathname is
   c:\Temp\converterTest\5540\_betriebsordnung-cd.doc
   c:\Temp\converterTest\5540\betriebsordnung-cd.html
HTMLConverterAgent: [TestDocument] Updating MetaData finished.
...
```

Eine Fehlersituation ist dann aufgetreten, wenn die Zeile

```
HTMLConverterAgent: [...] Updating Metadata finished.
```

nicht ausgegeben wird. Fehler werden in die Datei **err.out** und auf die temporäre HTML-Seite des erzeugten Verbundobjektes geschrieben.

Hinweis: Für Fehleranalysen ist in einem solchen Fall insbesondere die Zeile `HTMLConverterAgent: Running ...` aufschlußreich. In dieser Zeile wird der Aufruf ausgegeben, mit dem das externe Konvertierungsprogramm gestartet wird. Dieser Aufruf kann hinsichtlich seiner richtigen Funktionsweise manuell getestet werden.

In diesem Zusammenhang ist zu beachten, daß eine fehlerhafte Konvertierung beim erstmaligen Anlegen eines Verbundobjektes mit der Option *generieren mit Konverter* bewirkt, daß das dynamische Attribut “Converter” nicht gesetzt wird. Dies kann nach Beseitigung der Fehlerursache gegebenenfalls manuell nachgeholt werden.

B.3 Funktionsweise

Der HTMLConverter-Agent ist in den Erstellungsprozeß eines Verbundobjekts integriert und verwendet für den Konvertierungsvorgang ein externes Konvertierungsprogramm.

Hinsichtlich der Aktivierung des externen Konvertierungsprogramms ist der HTMLConverter-Agent nicht festgelegt, d. h. es kann – unter Beachtung der im Abschnitt B.1 “Installation” auf Seite 218 genannten Einschränkungen – ein beliebiges Programm zur Konvertierung eingesetzt werden. Das Ergebnis der Konvertierung und somit auch die Qualität der generierten Zieldateien hängen vom gewählten Konvertierungsprogramm und dessen Konfiguration ab.

Konvertierungsprozeß

Wenn im Pflegesystem ein Verbundobjekt erstellt bzw. nach Bearbeitung wieder zurückgegeben wird, spricht der Server über das VIP’ContentManager API den HTMLConverter-Agent an. Dieser überprüft beim Erstellen des Verbundobjekts, ob die Option *generieren mit Konverter* im Dialog *Neues Objekt anlegen* aktiviert wurde bzw. prüft beim Zurückgeben, ob das aktuelle Verbundobjekt durch einen Konverter übersetzt werden soll (siehe dazu auch den Abschnitt “Anlegen eines automatisch generierten Verbundobjekts” auf Seite 229).

Die folgende Abbildung veranschaulicht den Ablauf des automatischen Konvertierungsprozesses:

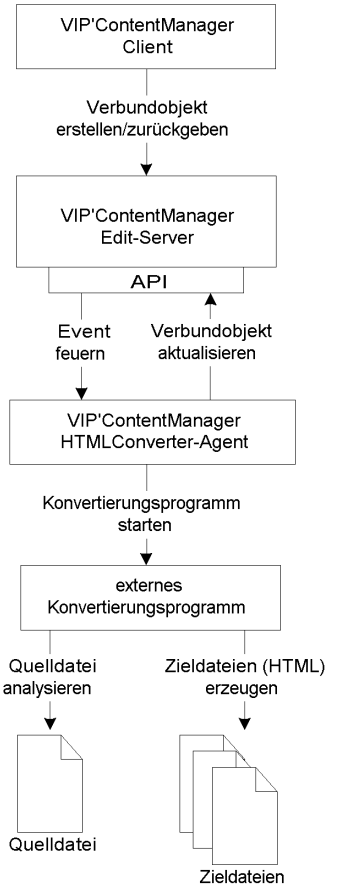

Abb. 67 – Der automatische Konvertierungsprozeß

Vor der automatischen Konvertierung besteht das Verbundobjekt aus der Quelldatei und einer temporären HTML-Seite. Diese HTML-Seite wird durch die Aktualisierung des Verbundobjekts im letzten Schritt des Konvertierungsprozesses ersetzt. Sollte während des Konvertierungsprozesses ein Fehler auftreten, wird die temporäre HTML-Seite mit einer entsprechenden Fehlermeldung versehen.

Die Konvertierung erfolgt im asynchronen Modus. Der Client generiert zunächst nur ein Verbundobjekt mit einer temporären HTML-Seite und meldet das Objekt anschließend als eingestellt. Die Konvertierung ist zu diesem Zeitpunkt noch nicht

abgeschlossen. Sie wird im Hintergrund weiter vollzogen, und die Aktualisierung des Verbundobjekts erfolgt nach und nach. Um den aktuellen Zustand des Verbundobjekts beim Konvertierungsprozeß zu erfragen, muß die entsprechende Seite neu vom Server abgerufen werden.

Sämtliche Aktionen des HTMLConverter-Agent werden in den Protokoll- und Fehlerdateien des Pflegesystems gespeichert. Im Fall einer fehlerhaften Konvertierung sollten diese Dateien zuerst überprüft werden. Eine Fehlermeldung wird ebenfalls auf der temporären HTML-Seite ausgegeben, die zur Überprüfung herangezogen werden kann.

Anlegen eines automatisch generierten Verbundobjekts

Das Anlegen eines automatisch generierten Verbundobjekts erfolgt über den Dialog *Neues Objekt anlegen*. Die folgende Abbildung zeigt diesen Dialog mit der Option *generieren mit Konverter*, die beim Erstellen eines Verbundobjekts zur Verfügung steht, sofern der HTMLConverter-Agent aktiviert wurde (siehe dazu den Abschnitt “Einstellungen für den Einsatz des HTMLConverter-Agent” auf Seite 218).

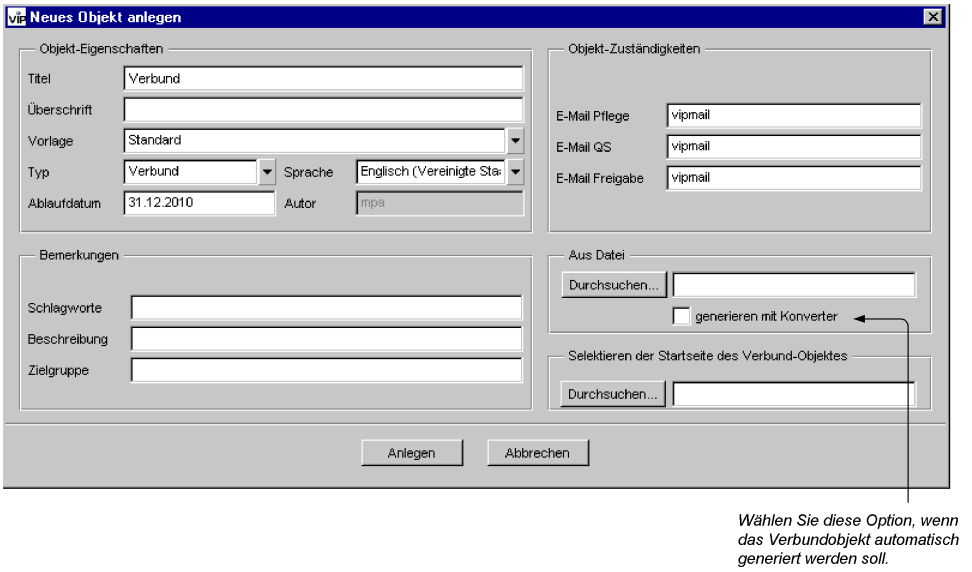

Abb. 68 – Die Option *generieren mit Konverter* im Dialog *Neues Objekt anlegen*

Wenn beim Erstellen des Verbundobjekts die Option *generieren mit Konverter* aktiviert wurde, ruft der HTMLConverter-Agent ein externes Konvertierungsprogramm auf, das die Konvertierung durchführt. Das Programm analysiert die Quelldatei und konvertiert sie schließlich mit Hilfe vordefinierter Layoutvorschriften in HTML-Seiten bzw. -Dateien. An welchen Stellen neue HTML-Seiten generiert werden, wird durch die Konverterregeln festgelegt. Der letzte Schritt der automatischen Konvertierung besteht in der Aktualisierung des Verbundobjekts mit den neu generierten Zieldateien durch den HTMLConverter-Agent.

Die über den Dialog *Neues Objekt anlegen* wählbare Option *generieren mit Konverter* wird im Verbundobjekt selbst abgespeichert. Zu diesem Zweck wird das dynamische Attribut “Converter” verwendet. Dieses Attribut kann per Mausklick auf *Attribute* im Metadatenfenster des entsprechenden Objektes nachträglich deaktiviert bzw. wieder aktiviert werden. Eine automatische Konvertierung der Quelldatei erfolgt nur dann, wenn das Attribut “Converter” den Wert “autogenerated;” enthält, wie in der folgenden Abbildung dargestellt.

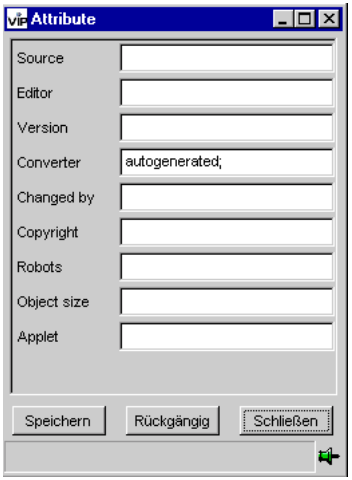

Abb. 69 – Das Attribut “Converter”

B.4 Testprogramm

Ein im Lieferumfang enthaltenes Testprogramm, das in der Datei **vipserver.jar** abgelegt ist, kann verwendet werden, um die Einstellungen in der Konfigurationsdatei **converter.properties** zu testen. Die Syntax für das Testprogramm lautet:

```
de.gauss.vip98.user.HTMLConverterAgent.ConverterTest ⇨
  ({source-file} {target-file}) | {source-directory}
```

Dabei haben die Platzhalter folgende Bedeutung:

`{source-file}`	Name und Pfad der Quelldatei
`{target-file}`	Name und Pfad der Zieldatei
`{source-directory}`	Pfad zu einem Verzeichnis, dessen Inhalt sowie dessen Unterverzeichnisse konvertiert werden sollen

Diese Syntax setzt voraus, daß sich der Java-Interpreter im entsprechenden Verzeichnispfad befindet und die benötigten Konverter-Klassen in der Umgebungsvariablen CLASSPATH enthalten sind. Das Programm sucht seine

Konfigurationsdatei **converter.properties** im aktuellen Verzeichnis. Dieses ist in der Regel nicht mit dem des Edit-Servers identisch. Nach erfolgreichem Test sollte deshalb die Konfigurationsdatei auf den Edit-Server übertragen werden.

Je nach Aufruf kann das Testprogramm in zwei unterschiedlichen Betriebsarten verwendet werden. Entweder wird genau eine Quelldatei in eine (oder mehrere) Zieldateien konvertiert, oder es werden alle konvertierbaren Dateien eines Verzeichnisses, inklusive der Unterverzeichnisse, in eine (oder mehrere) Zieldateien konvertiert. Die folgenden zwei Aufrufe sollen diese beiden Möglichkeiten beispielhaft veranschaulichen:

Aufruf für die Konvertierung einer Quelldatei in eine (oder mehrere) Zieldateien:

```
de.gauss.vip98.user.HTMLConverterAgent.ConverterTest ⇨
  c:\temp\myDocument.doc c:\temp\myDocument.html
```

Aufruf für die Konvertierung aller konvertierbaren Dateien eines Verzeichnisses in eine (oder mehrere) Zieldateien:

```
de.gauss.vip98.user.HTMLConverterAgent.ConverterTest c:\temp
```

Glossar

Adresse – siehe *URL*.

CSV-Tabellen – Comma Separated Value-Tabellen. CSV-Tabellen werden im VIP-System zur Speicherung von strukturierten Daten benutzt.

Dynamische Attribute – *siehe Special-Attribute*.

Edit-System – siehe *Pflegesystem*.

Extranet – Auf Internettechnologien basierte Informationsplattform für die Unternehmenskommunikation mit autorisierten externen Benutzern, z. B. Partnern oder Kunden.

Frameobjekt – Ein Objekttyp für ein Frameset.

Frame-Thema – Ein Frameobjekt, das gleichzeitig als Thema (zur inhaltlichen Organisation) verwendet wird. Siehe auch *Thema*.

Grafikobjekt – Eine Grafikdatei im Format JPEG, GIF, PNG oder einem anderen Format.

HTTP – HyperText Transfer Protocol. Ein Kommunikationsprotokoll zum Transfer von HTML-Seiten.

ISAPI – Internet Server API. Eine Programmierschnittstelle für den Microsoft Webserver (Internet Information Server).

Java – Von SUN-Microsystems entwickelte, objektorientierte Programmiersprache, die vor allem im Bereich der Internettechnologien genutzt wird. Sicherheitsaspekte und Plattformunabhängigkeit sind die Grundphilosophien von Java.

JDK – Java Development Kit.

LDAP – Lightweight Directory Access Protocol. Das LDAP basiert auf dem X.500-Standard und wird von den meisten großen Softwareherstellern unterstützt.

Metadaten – Jedem VIP-Objekt sind eine Reihe von Attributen (wie z. B. Ablaufdatum, Sprache) zugeordnet. Diese werden als Metadaten bezeichnet.

NSAPI – Netscape Server API. Eine Programmierschnittstelle für die Netscape Webserver.

Pflegesystem – Als Pflegesystem (oder auch Edit-System) wird der Bereich des VIP'ContentManager bezeichnet, in dem die Objekte einer Website angelegt und redaktionell bearbeitet werden.

Produktionssystem – Als Produktionssystem wird der Bereich des VIP'ContentManager bezeichnet,

der den Zugang zu den freigegebenen Seiten einer Website ermöglicht.

Proxy-Server – Ein Zwischenserver, der dazu dient, Anforderungen von einer Client-Anwendung, etwa einem Webbrowser, an einen anderen (oder mehrere andere) Server abzufangen. Wenn der Proxy-Server die Anforderung erfüllen kann, sendet er die angeforderten Daten an die Client-Anwendung zurück. Andernfalls leitet er die Anforderung an den spezifizierten Server weiter.

QS-System – Das QS-System des VIP'ContentManager dient der Qualitätssicherung der Objekte und damit der Website-Inhalte. Dieser Bereich stellt also die Kontrollinstanz zwischen dem Pflegesystem und dem Einsatz im Produktionssystem dar.

Rolle – Eine Zusammenstellung von Benutzern, ähnlich wie eine Benutzergruppe, für die bestimmte Zugriffsrechte definiert werden können. Die Benutzerrolle wird meistens aufgabenbezogen definiert, während Benutzergruppen in der Regel an Organisationseinheiten wie Abteilungen oder Projekte geknüpft sind.

SMTP – Simple Mail Transfer Protocol. Ein Protokoll für den Transfer von E-Mail-Nachrichten z. B. zwischen verschiedenen Servern.

Sonstiges-Objekt – Alle Objekte, die keinem der anderen Objekttypen entsprechen, werden als Sonstiges Objekt eingebunden. Beispielsweise zählen dazu Grafiken in anderen Formaten als die vom Objekttyp Grafik unterstützten.

Special-Attribute – Spezielle Metadaten, die für jeden Objekttyp unterschiedlich definiert werden können.

TCP/IP – Transmission Control Protocol/Internet Protocol. Basisprotokoll für die Übertragung von Daten im Internet.

Thema – Eine Kombination aus einer HTML-Seite zur direkten Darstellung von Informationen und einem Verzeichnis für die Aufnahme von untergeordneten Objekten. Die Themen werden im Objektbaum als Knotenpunkt dargestellt und dienen damit auch zur Strukturierung der Website.

Typ – Bezeichnet die spezifische Art des jeweiligen Objekts. Der Objekttyp wird beim Anlegen des Objekts festgelegt und kann bei bestimmten Objekttypen nachträglich verändert werden.

URL – Uniform Resource Locator. Eine eindeutige Adresse im World Wide Web.

VIP-Server – Es gibt drei parallel arbeitende VIP-Server für das Pflege-, QS- und Produktionssystem sowie einen VIP-Server für das Administrationssystem.

Web-Repository – Als Web-Repository wird der Bereich bezeichnet, in dem sämtliche Objekte einer Website durch das VIP-System abgelegt und verwaltet werden.

Webtechnologie – Client/Server-Technologie, die auf TCP/IP basiert. Der Vorteil liegt in dem offenen Standard, wodurch sich heterogene Systeme verwirklichen lassen.

Index

A

Anmelden (im Administrationssystem) 124
Apache
  Zugriffsschutz 74
  Zugriffsschutz unter Solaris 75
Asynchrone Konvertierung 228
Attribut
  Converter 230
Authentifizierungsmethode 70
autogenerated 230

B

Baumoperationen 191
Benutzer-Administration 133
  Benutzer löschen 136
  Funktionsbereiche 140
  Gruppenzuordnung 137
  Neuen Benutzer anlegen 134
  Rollenzuordnung 138
  Standardzugriffsrechte 139
  Zugang sperren 135, 141
Benutzerkennungen
  Hinweise zu 76
Benutzeroberflächen 11

C

client_config.properties 58
CSV-Treiber 92

D

Datei- und Verzeichnisstruktur 20
  Websites 25
Daten
  wiederherstellen eines früheren Bestands 113
Datenbankanbindung
  Hinweise 89
  Konfiguration 93–101
  Systemüberblick 91
  Umstellung (Migration) 89
  unterstützte Datenbanksysteme 94
  Vorgehen im Überblick 94
Datenbankkonfiguration
  DB2 104
  JDBC- bzw. JDBC-ODBC-Datenquellen 102
  Microsoft SQL Server 6.5 105
  Microsoft SQL Server 7.0 106
  Oracle 8 103
Datensicherung 110–113
  Durchführung 110
  Runlevel "Backup" 111
  Verhalten im Fehlerfall 113
DBC-Parameter 98
DefaultContent-Agent 209
  arbeiten mit 212
  Konfiguration 210
directory.properties 79, 160
  allgemeine Einstellungen 82
  Suchkontext-Einstellungen 85
DiskSpace-Agent 115
  Konfiguration 117

F

Funktionsbereiche 140, 163

G

generieren mit Konverter 230
generieren mit Konverter (Option) 227
Gruppen-Administration 142
  Benutzerzuordnung 145
  Gruppe löschen 144
  Neue Gruppe anlegen 143
Gruppenrollen 187, 194

H

Hauptspeicheranforderung
  verändern 121
HTMLConverter-Agent 217
  Funktionsweise 227–231
  Konfiguration 219–226
  Registrierung 218
httpd.conf 74

I

Installation 33–49
  Installationsvorgang 33
  Serverlizenz 49
  Voraussetzungen 31
ISAM-Treiber 92
ISAPI-Filter 70
IT-Strukturen 11

J

JDBC-Datenquellen 102
JDBC-Treiber 92

K

Konfiguration 55–75
  Arbeitsplatz-Voreinstellungen 55
  Bearbeitungsprogramme 55
  Client-Installation 58
  Datenbankanbindung 93–101
  DefaultContent-Agent 210
  DiskSpace-Agent 117
  HTMLConverter-Agent 219
  LDAP-Anbindung 76–88
  SetExecutable-Agent 114
  Webserver 59
  Zugriffsschutz 60–62, 64–75
Konfigurationsdateien
  client_config.properties 58
  directory.properties 79
  httpd.conf 74
  linux_editors.properties 55
  obj.conf 72
  pathlist.txt 64
  vipauth.ini 67, 68
  windows_editors.properties 55
Konfigurationsdateien (Datenbankanbindung)
  websites.properties 95
Konfigurationsdateien (HTMLConverter-Agent)
  converter.properties 219–224
  serverAgents.properties 218
Konvertierung
  asynchroner Modus 228
Konvertierungsprogramm (extern) 217
Konvertierungsprozeß 227–229

L

LDAP 160
  Abgleich durchführen 160
  Konfiguration 76–88
  Objektklassen und Attribute 77–78
linux_editors.properties 55
Lizenz 49

M

MS IIS 4.0
  Zugriffsschutz 68

N

Netscape Enterprise Server
  Zugriffsschutz 72

O

obj.conf 72
Objekte anlegen
  mit Option “direkte Freigabe” 164
  mit Option “HTML-Tag einfügen” 166
  mit Option “VIP-Objekt einfügen” 166
  mit zugeordnetem Funktionsbereich 163
Objektinformationen (Datenbankanbindung) 90
Objekttyp
  Verbundobjekt 217

ODBC-Datenquellen 102

P

Parameter (HTMLConverter-Agent)
- arg1 223
- arg2 223
- converterClassName 223
- debugOn 222
- env1 224
- env2 224
- maxSourceFileLength 222
- secureConvert 222
- synchronizedConvert 221
- tempDir 220
- tempDirRemove 220
- tempDirUseSubdir 220
- timeout 221
- validExtensions 221

Paßwörter
- Hinweise zu 76, 125, 135

pathlist.txt 64

Property-Dateien 22

R

Registrierung
- HTMLConverter-Agent 218

Rollen-Administration 148
- Benutzerzuordnung 150
- Neue Rolle anlegen 149
- Rolle löschen 150
- Standardzugriffsrechte 152

Runlevel "Backup" 111

S

Serverlizenz 49

Serverprozesse 19

SetExecutable-Agent
- Konfiguration 114

Speicherstrategie
- Einstellung 107–109

Suchkontext (in LDAP) 85

Systemadministration 154

Systemarchitektur 17
- Abbildung 18

T

Testprogramm (HTMLConverter-Agent) 231

V

Verändern
- maximale Hauptspeicheranforderung 121

Verbundobjekt
- der Objekttyp 217

Vererbung 171

Verzeichnisdienste 160
- Abgleich durchführen 160

Verzeichnisse 20

VIP'DBC
- Architektur 91

vipauth.ini 67, 68

VIP-Server
- herunterfahren über Skript-Datei 157
- installieren 33
- starten 50

Voreinstellungen 55
- Bearbeitungsprogramme 55
- Client-Installation 58

Vorrangsregeln 175

W

Web Content Management System 11

Webserver
- Konfiguration 59

Website
- Verzeichnisstruktur 25

Website-Administration 126
- Benutzerzuordnung 132
- Gruppenzuordnung 130
- Rollenzuordnung 131
- Website anlegen 128
- Website-Administratoren 129

websites.properties

Konfigurationsdateien
(Datenbankanbindung) 95
Wiederherstellen
eines früheren Datenbestands 113
frühere Objektversion 59
windows_editors.properties 55

Z

Zugriffskontrolle 169
Zugriffsrechte 169
aufgabenspezifische 184
einstellen 177
für “alle Benutzer” einstellen 182
im Produktionssystem 182
objektspezifische 170
Recht auf Änderung 190
standardmäßig 174
Vererbungsprinzip 171
Vorrangsregeln 175
Zugriffsschutz 60–75
Authentifizierungsmethode (MS IIS) 70
Funktionsweise 60
ISAPI-Filter (MS IIS) 70
Konfiguration 64–75
Microsoft-Webserver 67
MS IIS 4.0 68
Netscape Enterprise Server 72
Systemüberblick 61